Según una alta funcionaria de seguridad cibernética, es posible que el gobierno de Estados Unidos no pueda evitar otro ataque cibernético global como WannaCry.

Jeanette Manfra, directora asistente de ciberseguridad de la Agencia de Seguridad de la Ciberseguridad e Infraestructura (CISA) de Seguridad Nacional, dijo en el escenario de TechCrunch Disrupt SF, que el ciberataque WannaCry de 2019, que afectó a cientos de miles de computadoras en todo el mundo, fue un desafío único, ya que se extendió muy rápido.

> *«No sé si alguna vez podríamos evitar algo así. Simplemente tenemos algo que se manifiesta completamente como un gusano. Creo que los autores originales no esperaban probablemente ese tipo de impacto»,* dijo Manfra.

El ataque cibernético WannaCry fue el primer gran incidente de seguridad global en años. Se cree que los hackers asociados con Corea del Norte utilizaron un conjunto de herramientas de piratería altamente clasificadas que solo unas semanas antes habían sido robadas de la Agencia de Seguridad Nacional y publicadas en línea.

Las herramientas permitieron que cualquiera que las usara infectara miles de computadoras vulnerables con una puerta trasera. Esa «backdoor» se utilizó para entregar la carga útil de WannaCry, que bloqueaba a los usuarios de sus propios archivos a menos que se pagara un rescate.

Para colmo, WannaCry tenía propiedades de gusano, lo que le permitía extenderse por medio de la red y dificultar su contención.

Aunque la Agencia de Seguridad Nacional nunca reconoció públicamente el robo de sus herramientas de piratería, Seguridad Nacional dijo en ese momento que los usuarios eran *«la primera línea de defensa»* contra la amenaza de WannaCry. Microsoft lanzó correcciones de seguridad semanas antes, pero muchos no habían instalado los parches.

«Actualizar sus parches habría evitado que una buena cantidad de personas fueran

víctimas», agregó Manfra. Sin embargo, los datos muestran que dos años después de los ataques, más de un millón de computadoras seguían siendo vulnerables al ransomware.

Manfra dijo que *«van a suceder cosas malas»*, pero que los esfuerzos para movilizar al gobierno y al sector privado pueden ayudar a combatir los ataques cibernéticos a medida que surjan.

> *«Afortunadamente, había una persona emprendedora que fue capaz de encontrar una forma de matarlo y no impactó tanto a Estados Unidos»,* dijo.

Marcus Hutchins, un ingeniero de ingeniería inversa de malware e investigador de seguridad, registró un nombre de dominio que encontró el código del ransomware que, cuando se registraba, actuaba como un *«interruptor de apagado»*, evitando que el ransomware se propagara.

Hutchins fue aclamado como un *«héroe accidental»* por sus esfuerzos. Hutchins y su colega, Jamie Hankins, pasaron una semana asegurándose de que el interruptor de matar se mantuviera activo, ayudando a prevenir millones de infecciones adicionales.

Los comentarios de Manfra se produjeron solo semanas después de que su departamento advirtiera sobre una nueva amenaza emergente planteada por BlueeKeep, una vulnerabilidad encontrada en Windows 7 y versiones anteriores, que según los expertos tiene la capacidad de desencadenar otro incidente global similar a WannaCry. BlueKeep puede explotarse para ejecutar código malicioso, como malware o ransomware.

Al igual que WannaCry, BLueKeep también tiene propiedades aptas para gusanos, lo que le permite extenderse a otras computadoras vulnerables en la misma red.

Se estima que un millón de dispositivos conectados a Internet son vulnerables a BlueKeep. Los investigadores de seguridad afirman que es solo cuestión de tiempo antes de que los atacantes desarrollen y utilicen un exploit BlueKeep para llevar un ataque cibernético

parecido a WannaCry.

Créditos de imagen: TechCrunch