El FBI elimina programa malicioso chino de miles de computadoras estadounidenses

-
- 15/1/2025

El Departamento de Justicia y el fbi dijeron el martes que habían eliminado el programa malicioso [*malware*] PlugX, patrocinado por China, de más de 4.200 computadoras y redes de Estados Unidos.

Jaqueado: según un expediente judicial, China pagó al grupo de piratas informáticos Mustang Panda, también conocido como Twill Typhoon, para que desarrollara programas maliciosos, como PlugX, con el fin de infectar, controlar y robar información de computadoras extranjeras.

Desde al menos 2014, los jáqueres de Mustang Panda se han infiltrado en miles de computadoras con Windows en EE UU, Europa y Asia. El expediente judicial explica:

> La investigación de varios años del fbisobre Mustang Panda ha confirmado que este grupo de jáqueres informáticos se ha infiltrado en los sistemas informáticos de numerosas organizaciones gubernamentales y privadas, incluyendo EE UU. Entre los objetivos extranjeros más importantes figuran compañías navieras europeas en 2024, varios gobiernos europeos de 2021 a 2023, (…) grupos disidentes chinos de todo el mundo y gobiernos de todo el Indopacífico (p. ej., Taiwán, Hong Kong, Japón, Corea del Sur, Mongolia, India, Myanmar, Indonesia, Filipinas, Tailandia, Vietnam y Pakistán).

El expediente judicial explica que el programa malicioso puede propagarse fácilmente a otras computadoras a través de dispositivos usb. Los propietarios de computadoras infectadas a menudo no saben que su dispositivo ha sido jaqueado.

Comprometida: en septiembre de 2023, la empresa privada francesa de ciberseguridad Sekoia.io comprometió la dirección IP que PlugX utilizaba para comunicarse con el servidor de mando y control de Mustang Panda.

Desde entonces, el programa malicioso PlugX en dispositivos estadounidenses puede haber intentado contactar con el servidor del grupo de piratas informáticos 45.000 veces diferentes, según el expediente judicial.

Eliminado: en agosto de 2024, el Departamento de Justicia y elfbi obtuvieron nueve órdenes judiciales que les autorizaban a utilizar el comando de autodestrucción de PlugX para eliminarlo de los dispositivos en EE UU.

• Un total de 4.258 sistemas estadounidenses fueron limpiados del programa malicioso antes de que expirara la orden final el 3 de enero.

Dependencia: a medida que EE UU depende cada vez más de la cibertecnología para fines gubernamentales, militares, empresariales y cotidianos, China se está volviendo cada vez más hábil para jaquear esa tecnología. La profecía bíblica advierte que esta dependencia es peligrosa.

Más información: lea “Los ciberataques exponen nuestro frágil mundo”.