laTrompette

Le FBI efface des logiciels malveillants chinois de milliers d'ordinateurs américains

-
- 15/01/2025

Le ministère américain de la Justice et le FBI ont déclaré mardi qu'ils avaient retiré le malware PlugX, sponsorisé par la Chine, de plus de 4 200 ordinateurs et réseaux aux États-Unis.

Piraté : Selon un document judiciaire, la Chine a payé le groupe de hackers Mustang Panda, également connu sous le nom de Twill Typhoon, pour développer des logiciels malveillants, comme PlugX, afin d'infecter, de contrôler et de voler des informations sur des ordinateurs étrangers.

Depuis au moins 2014, les pirates de Mustang Panda ont infiltré des milliers d'ordinateurs fonctionnant sous Windows aux États-Unis, en Europe et en Asie. Selon le dossier du tribunal :

> L'enquête pluriannuelle du FBI sur Mustang Panda a confirmé que ce groupe de pirates informatiques a infiltré les systèmes informatiques de nombreuses organisations gouvernementales et privées, y compris aux États-Unis. Les cibles étrangères significatives comprennent les compagnies maritimes européennes en 2024, plusieurs gouvernements européens de 2021 à 2023, […] des groupes de dissidents chinois dans le monde entier, et des gouvernements à travers l'Indo-Pacifique (par exemple, Taïwan, Hong Kong, Japon, Corée du Sud, Mongolie, Inde, Myanmar, Indonésie, Philippines, Thaïlande, Vietnam et Pakistan).

Le dossier judiciaire explique que le logiciel malveillant peut facilement se propager à d'autres ordinateurs par l'intermédiaire de périphériques USB. Les propriétaires d'ordinateurs infectés ignorent souvent que leur appareil a été piraté.

Infiltration : En septembre 2023, la société française de cybersécurité privée Sekoia.io a découvert l'adresse IP utilisée par PlugX pour communiquer avec le serveur de commande et de contrôle de Mustang Panda.

Depuis lors, le logiciel malveillant PlugX sur les appareils américains aurait essayé de contacter le serveur du groupe de hackers 45 000 fois, selon le dossier judiciaire.

Supprimé : En août 2024, le ministère américain de la Justice et le FBI ont obtenu neuf mandats les autorisant à utiliser la commande d'autodestruction de PlugX pour l'éliminer des appareils aux États-Unis.

• Au total, 4 258 systèmes américains ont été nettoyés du logiciel malveillant avant l'expiration du mandat final le 3 janvier.

Dépendance : Alors que les États-Unis deviennent de plus en plus dépendants de la technologie cybernétique pour les

besoins gouvernementaux, militaires, commerciaux et quotidiens, la Chine devient de plus en plus habile à pirater cette technologie. La prophétie biblique nous avertit que cette dépendance est dangereuse.

En savoir plus : Lisez « *Les cyberattaques révèlent la fragilité de notre monde* ».