FBI löscht chinesische Malware von Tausenden von amerikanischen Computern

-
- 15.01.2025

Das Justizministerium und das fbi gaben am Dienstag bekannt, dass sie die von China gesponserte PlugX-Malware von über 4200 Computern und Netzwerken in den Vereinigten Staaten entfernt haben.

Gehackt: Laut einer Gerichtsakte hat China die Hackergruppe Mustang Panda, auch bekannt als Twill Typhoon, dafür bezahlt, Malware wie PlugX zu entwickeln, um ausländische Computer zu infizieren, zu kontrollieren und Informationen zu stehlen.

Mindestens seit 2014 haben die Hacker von Mustang Panda Tausende von Windows-basierten Computern in den USA, Europa und Asien infiltriert. Die Gerichtsakte erklärt:

> Die mehrjährigen Ermittlungen des fbi gegen Mustang Panda haben bestätigt, dass diese Gruppe von Computerhackern in die Computersysteme zahlreicher staatlicher und privater Organisationen eingedrungen ist, auch in den Vereinigten Staaten. Zu den wichtigsten ausländischen Zielen gehören europäische Reedereien im Jahr 2024, mehrere europäische Regierungen von 2021 bis 2023 … weltweite chinesische Dissidentengruppen und Regierungen im gesamten indopazifischen Raum (z.B. Taiwan, Hongkong, Japan, Südkorea, Mongolei, Indien, Myanmar, Indonesien, Philippinen, Thailand, Vietnam und Pakistan).

In der Gerichtsakte wird erklärt, dass sich die Malware überUSB-Geräte leicht auf andere Computer verbreiten kann. Die Besitzer von infizierten Computern wissen oft nicht, dass ihr Gerät gehackt worden ist.

Kompromittiert: Im September 2023 kompromittierte das französische private Cybersicherheitsunternehmen Sekoia.io die IP-Adresse, die PlugX für die Kommunikation mit dem Befehls- und Kontrollserver von Mustang Panda verwendete.

Seitdem hat die PlugX-Malware auf US-Geräten möglicherweise 45 000 Mal versucht, den Server der Hackergruppe zu kontaktieren, wie aus der Gerichtsakte hervorgeht.

Gelöscht: Im August 2024 erhielten das US-Justizministerium und das fbi neun Durchsuchungsbefehle, die sie ermächtigten, den Selbstzerstörungsbefehl von PlugX zu verwenden, um es von Geräten in den USA zu entfernen.

• Insgesamt wurden 4258 amerikanische Systeme von der Malware gesäubert, bevor der letzte Haftbefehl am 3. Januar ablief.

Abhängigkeit: Während die USA in den Bereichen Regierung, Militär, Wirtschaft und Alltag immer mehr von der Cybertechnologie abhängig werden, wird China immer geschickter darin, diese Technologie zu hacken. Die biblische Prophezeiung warnt davor, dass diese Abhängigkeit gefährlich ist.

Erfahren Sie mehr: Lesen „Cyberattacken offenbaren unsere zerbrechliche Welt.“