FBI deletes Chinese PlugX malware from thousands of US computers

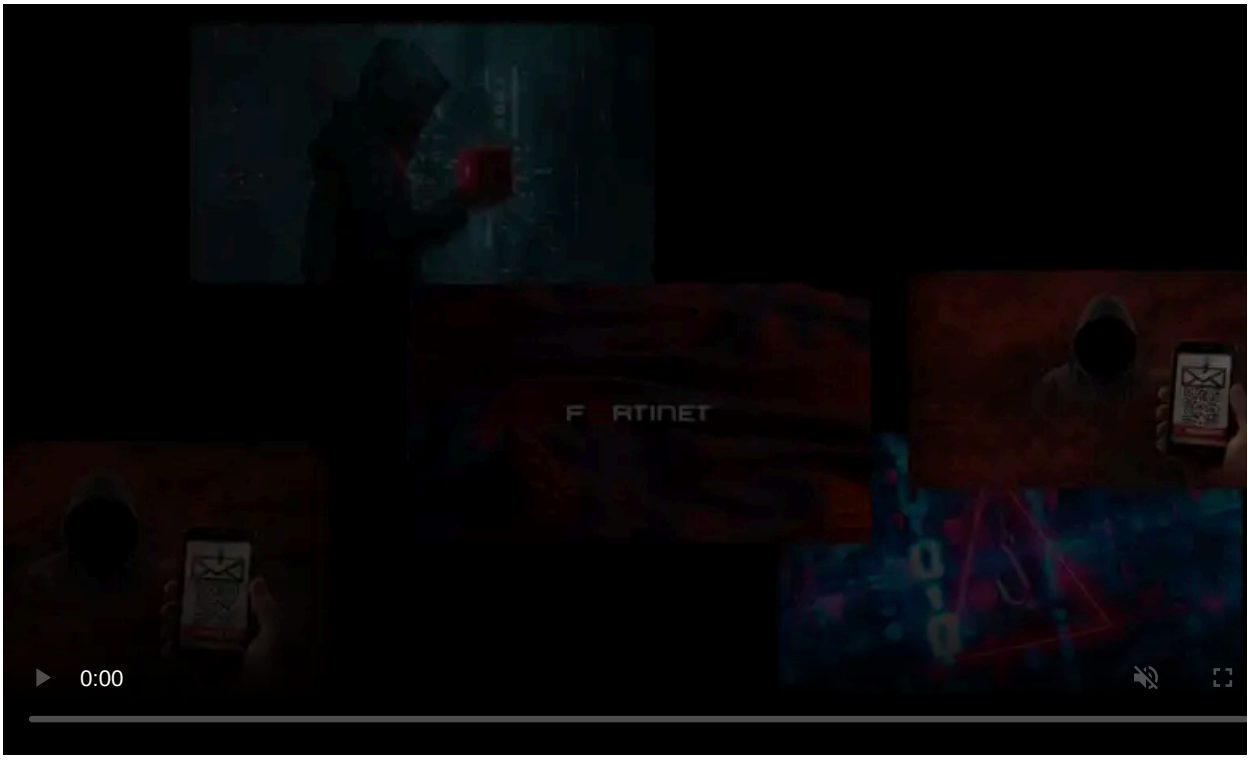
By Sergiu Gatlan

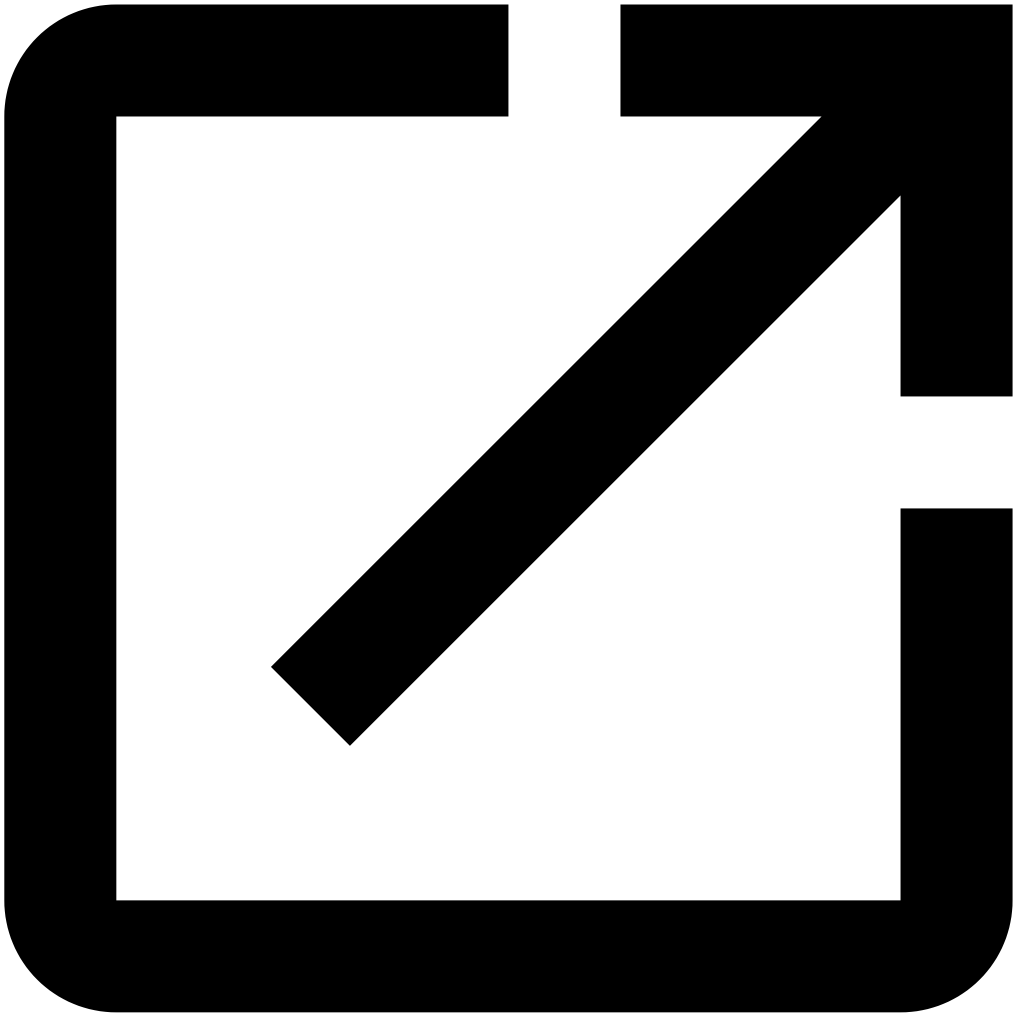
Published: 2025-01-14 · Archived: 2026-04-05 21:13:24 UTC

The U.S. Department of Justice announced today that the FBI has deleted Chinese PlugX malware from over 4,200 computers in networks across the United States.

The malware, controlled by the Chinese cyber espionage group Mustang Panda (also tracked as Twill Typhoon), infected thousands of systems using a PlugX variant with a wormable component that allowed it to spread through USB flash drives.

According to court documents, the list of victims targeted using this malware includes "European shipping companies in 2024, several European Governments from 2021 to 2023, worldwide Chinese dissident groups, and governments throughout the Indo-Pacific (e.g., Taiwan, Hong Kong, Japan, South Korea, Mongolia, India, Myanmar, Indonesia, Philippines, Thailand, Vietnam, and Pakistan)."


F RTINET
0:00



"Once it has infected the victim computer, the malware remains on the machine (maintains persistence), in part by creating registry keys which automatically run the PlugX application when the computer is started," the affidavit reads. "Owners of computers infected by PlugX malware are typically unaware of the infection."

This court-authorized action is part of a global takedown operation led by French law enforcement and cybersecurity company Sekoia. The operation started in July 2024, when French police and Europol removed the remote access trojan malware from infected devices in France.

"In August 2024, the Justice Department and FBI obtained the first of nine warrants in the Eastern District of Pennsylvania authorizing the deletion of PlugX from U.S.-based computers," the Justice Department said today.

"The last of these warrants expired on Jan. 3, 2025, thereby concluding the U.S. portions of the operation. In total, this court-authorized operation deleted PlugX malware from approximately 4,258 U.S.-based computers and networks."

The command sent to infected computers by the FBI told the PlugX malware:

1. Delete the files created by the PlugX malware on the victim's computer,
2. Delete the PlugX registry keys used to automatically run the PlugX application when the victim computer is started,
3. Create a temporary script file to delete the PlugX application after it is stopped,
4. Stop the PlugX application and
5. Run the temporary file to delete the PlugX application, delete the directory created on the victim computer by the PlugX malware to store the PlugX files, and delete the temporary file from the victim computer.

The FBI is now notifying the owners of U.S.-based computers that have been cleaned of the PlugX infection through their internet service providers and says the action didn't collect information from or impact the disinfected devices in any way.

Cybersecurity firm Sekoia previously discovered a botnet of devices infected with the same PlugX variant, taking control of its command and control (C2) server at 45.142.166[.]112 in April 2024. Sekoia said that, over six months, the botnet's C2 server received up to 100,000 pings from infected hosts daily and had 2,500,000 unique connections from 170 countries.

PlugX has been used in attacks since at least 2008, mainly in cyber espionage and remote access operations by groups linked to the Chinese Ministry of State Security. Multiple threat groups have used it to target government, defense, technology, and political organizations, primarily in Asia and later expanding to the rest of the world.

Some PlugX builders have also been detected online, and some security researchers believe the malware's source code leaked around 2015. This, combined with the tool's multiple updates, makes it very difficult to attribute the malware's development and use in attacks to a specific threat actor or agenda.

The PlugX malware features extensive capabilities, including collecting system information, uploading and downloading files, logging keystrokes, and executing commands.

Source: https://www.bleepingcomputer.com/news/security/fbi-deletes-chinese-plugx-malware-from-thousands-of-us-computers/