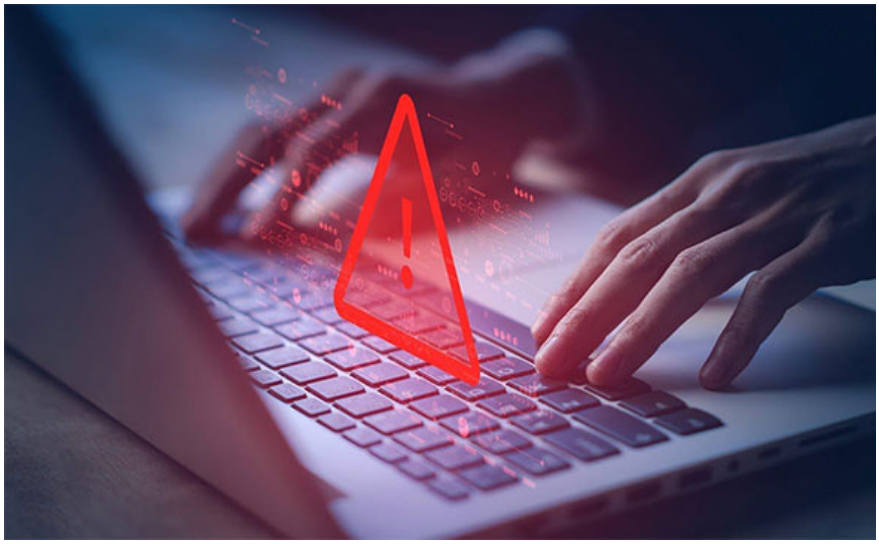
FBI 'eliminates' malware that affected 2.5 million PCs

A piece of malware originating from China has now been contained after the FBI obtained a court order to remove the malicious code from thousands of Windows computers.

A piece of malware originating from China has now been stopped after the FBI obtained a court order to remove the malicious code from thousands of Windows computers.

The agency has successfully ended the reign of the PlugX malware strain in the United States, which is believed to have affected more than 2.5 million devices globally through the route of infiltration via infected USB drives.

The US Department of Justice has previously worked closely with the FBI and confirmed that it has received court approval to remove the malware from nearly 4,260 computers and networks in the United States as of January 14, 2025. With the resolution announced, the FBI will notify the owners of the infected machines through their internet service providers.



This is just one example of how serious cybersecurity risks are being controlled by U.S. regulators. However, officials have also noted the importance of cybersecurity in the current climate. The U.S. Department of Justice detailed that the attackers were a Chinese state-sponsored private hacker group called 'Mustang Panda,' which developed a unique version of the PlugX malware for the ongoing campaign.

PlugX first appeared in 2008 as a backdoor that allowed attackers to secretly take control of Windows computers. In 2020, the malware was updated to include the ability to infect USB drives as well as connected PCs.

This led PlugX to be described as "wormable" malware that could be transmitted between computers via infected peripherals.

French cybersecurity firm Sekoia later found that Mustang Panda did not have the resources to support the number of machines infected with PlugX malware, and eventually abandoned the project. Similarly, antivirus vendor Sophos observed several instances of PlugX infections originating from a single source IP address. In September 2023, in partnership with Sekoia, the cybersecurity vendor paid just $7 for access to the IP addresses and infected machines. Further investigation later uncovered a self-destruct command in the PlugX code.

In July 2024, law enforcement in France authorized the use of a self-destruct mechanism to remediate infected machines. Since then, 22 other countries have implemented similar measures.

While it's unclear how entities in the United States plan to remove the malware from domestic PCs, the FBI testified in an affidavit that it tested this self-erasing command, confirming that it only removed the malware and did not affect any other functions of the device or transfer any other invalid code.