Justice Department and FBI Conduct International Operation to Delete Malware Used by China-Backed Hackers

justice.gov/opa/pr/justice-department-and-fbi-conduct-international-operation-delete-malware-used-china-backed

January 14, 2025

Press Release

Tuesday, January 14, 2025

For Immediate Release
Office of Public Affairs

Court-Authorized Operation Removes PlugX Malware from More Than 4,200 Infected U.S. Computers

Note: View the affidavit here.

The Justice Department and FBI today announced a multi-month law enforcement operation that, alongside international partners, deleted “PlugX” malware from thousands of infected computers worldwide. As described in court documents unsealed in the Eastern District of Pennsylvania, a group of hackers sponsored by the People’s Republic of China (PRC), known to the private sector as “Mustang Panda” and “Twill Typhoon,” used a version of PlugX malware to infect, control, and steal information from victim computers.

According to court documents, the PRC government paid the Mustang Panda group to, among other computer intrusion services, develop this specific version of PlugX. Since at least 2014, Mustang Panda hackers then infiltrated thousands of computer systems in campaigns targeting U.S. victims, as well as European and Asian governments and businesses, and Chinese dissident groups. Despite previous cybersecurity reports, owners of computers still infected with PlugX are typically unaware of the infection. The court-authorized operation announced today remediated U.S.-based computers infected with Mustang Panda’s version of PlugX.

“The Department of Justice prioritizes proactively disrupting cyber threats to protect U.S. victims from harm, even as we work to arrest and prosecute the perpetrators,” said Assistant Attorney General Matthew G. Olsen of the Justice Department’s National Security Division. “This operation, like other recent technical operations against Chinese and Russian hacking groups like Volt Typhoon, Flax Typhoon, and APT28, has depended on strong partnerships to successfully counter malicious cyber activity. I commend partners in the French government and private sector for spearheading this international operation to defend global cybersecurity.”

“Leveraging our partnership with French law enforcement, the FBI acted to protect U.S. computers from further compromise by PRC state-sponsored hackers,” said Assistant Director Bryan Vorndran of the FBI’s Cyber Division. “Today’s announcement reaffirms the FBI’s dedication to protecting the American people by using its full range of legal authorities and technical expertise to counter nation-state cyber threats.”

“This wide-ranging hack and long-term infection of thousands of Windows-based computers, including many home computers in the United States, demonstrates the recklessness and aggressiveness of PRC state-sponsored hackers,” said U.S. Attorney Jacqueline Romero for the Eastern District of Pennsylvania. “Working alongside both international and private sector partners, the Department of Justice’s court-authorized operation to delete PlugX malware proves its commitment to a ‘whole-of-society’ approach to protecting U.S. cybersecurity.”

“The FBI worked to identify thousands of infected U.S. computers and delete the PRC malware on them. The scope of this technical operation demonstrates the FBI’s resolve to pursue PRC adversaries no matter where they victimize Americans,” said Special Agent in Charge Wayne Jacobs of the FBI Philadelphia Field Office.

The international operation was led by French law enforcement and Sekoia.io, a France-based private cybersecurity company, which had identified and reported on the capability to send commands to delete the PlugX version from infected devices. Working with these partners, the FBI tested the commands, confirmed their effectiveness, and determined that they did not otherwise impact the legitimate functions of, or collect content information from, infected computers. 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 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 FBI, through the victims' internet service providers, is providing notice to U.S. owners of Windows-based computers affected by this court-authorized operation.

The FBI's Philadelphia Field Office and Cyber Division, the U.S. Attorney's Office for the Eastern District of Pennsylvania, and the National Security Cyber Section of Justice Department's National Security Division led the domestic disruption operation. This operation would not have been successful without the valuable collaboration of to the Cyber Division of the Paris Prosecution Office, French Gendarmerie Cyber Unit C3N, and Sekoia.io.

The FBI continues to investigate Mustang Panda's computer intrusion activity. If you believe you have a compromised computer or device, please visit the FBI's Internet Crime Complaint Center (IC3). You may also contact your local FBI field office directly. The FBI strongly encourages the use of anti-virus software as well as the application of software security updates to help prevent reinfection.

Updated January 24, 2025

Topic

National Security

Press Release Number: 25-50