1-The Washington Post-China suspected of breaching

China suspected of breaching U.S. Postal Service computer networks

Chinese government hackers are suspected of breaching the computer networks of the United States Postal Service, compromising the data of more than 800,000 employees — including the postmaster general's.

The intrusion was discovered in mid-September, said officials, who declined to comment on who was thought to be responsible *[Deny]*. The FBI is leading the investigation into the hack.

The news, announced by U.S. Postal Service, came as President Obama arrived Monday in Beijing for high-level talks with his counterpart, President Xi Jinping, as well as for an economic summit.

The Chinese government has consistently denied accusations that it engages in cybertheft and notes that Chinese law prohibits cybercrime. But China has been tied to several recent intrusions, including one into the computer systems of the Office of Personnel Management and another into the systems of a government contractor, USIS , that conducts security-clearance checks.

The intrusion into the USPS, officials said, was carried out by a sophisticated actor who did not appear to be interested in identity theft or credit card fraud.

“It is an unfortunate fact of life these days that every organization connected to the Internet is a constant target for cyber intrusion activity,” Postmaster General Patrick Donahoe said in a statement. “The United States Postal Service is no different. Fortunately, we have seen no evidence of malicious use of the compromised data and we are taking steps to help our employees protect against any potential misuse of their data.” *[Rebuild]*

The compromised data included names, dates of birth, Social Security numbers, addresses, dates of employment and other information, officials said. The data of every employee were exposed.

No customer credit card information from post offices or online purchases at usps.com was breached, officials said.

While the OPM and USIS breaches involved data of people who had gone through security clearances and so could be useful to a foreign government seeking to gain access to individuals in sensitive government work, it is not clear why Postal Service employees would be of such interest.

Still, analysts said a federal agency such as USPS would make a logical espionage target for China. For one thing, the Chinese may be assuming that the postal service is more like theirs — a state-owned entity that has vast amounts of data on its citizens, said James A. Lewis, a cyber-policy expert at the Center for Strategic and International Studies. Second, he said, China would be interested in amassing large sets of data that can be analyzed for previously unknown links or insights.

“They’re just looking for big pots of data on government employees,” Lewis said. “For the Chinese, this is probably a way of building their inventory on U.S. persons for counterintelligence and recruitment purposes.”

Advertisement

Such data may also be helpful in non-cyber espionage, said Steven Chabinsky, a former FBI official and now chief risk officer for CrowdStrike, a cybersecurity firm. “It’s not all about hackers. Having information about real live people could help them with on-the-ground operations.”

The U.S. government has strongly urged the Chinese to refrain from hacking U.S. companies to steal corporate secrets that can benefit Chinese industries. This case appears to more closely resemble traditional espionage, similar to the kind the United States engages in with respect to China.

Story continues below advertisement

Still, “it’s perfectly appropriate for us to do everything we can to embarrass and punish the Chinese if they’re in our systems, whether or not we’re in theirs,” said former National Security Agency general counsel Stewart A. Baker. “It’s the case that the U.S. and Russia and other countries are much more cautious about getting caught because they think there are going to be consequences. It’s only the Chinese that think there are no consequences to getting caught.”

Advertisement

Although the Postal Service began planning to resolve the matter as soon as it was notified of the breach by the FBI and other federal agencies *[Rebuild]*, it did not begin steps needed to repair the breach until this past weekend. *[Disappointment]*

“Acting too quickly could have caused more data to be compromised,” Partenheimer said.

Story continues below advertisement

New safeguards were put in place over the weekend to try to prevent future compromises, *[Rebuild]* he said. That process caused intermittent system

outages and slowed the delivery of external e-mail, he said.

The Department of Homeland Security's Computer Emergency Readiness Team helped with the mitigation, as it did with the OPM and USIS hacks.

The Postal Service breach needs to be seen as part of a continuous series of efforts to target the government, experts say. "It shows the continuing proposition that no matter how many billions of dollars the federal government puts in place and no matter how many regulations U.S. agencies put in place, the federal government remains as vulnerable as the private sector," Chabinsky said. *[Disappointment, Worry]*

The breach also affected the data of customers who contacted the Postal Service Customer Care Center via phone or e-mail between Jan. 1 and Aug. 16, officials said. The data affected included names, e-mail addresses and phone numbers, but not social security numbers, they said. Officials said they did not believe customers needed to take any action as a result of that.

However, FBI spokesman Joshua Campbell said any suspected instances of identity theft should be reported to the FBI's Internet Crime Complaint Center at www.ic3.gov .

The postal service began notifying employees on Monday. *[Rebuild]* The agency is providing free credit-monitoring services for one year. *[Rebuild]*

House Committee on Oversight and Government Reform Committee Ranking Member Elijah E. Cummings (D-Md.) on Monday requested details on the intrusion. "The increased frequency and sophistication of cyber-attacks upon both public and private entities highlight the need for greater collaboration to improve data security," he said in a letter to Donahoe .

GiftOutline