theguardian

Chinese hackers break into US federal government employee database

News of attempt to target people who had applied for security clearances comes as John Kerry attends Sino-American summit

Dominic Rushe in New York
theguardian.com, Thursday 10 July 2014 12.32 EDT

John Kerry speaks at a press conference following the end of talks at the US-China Strategic and Economic Dialogue in Beijing. Photograph: Greg Baker/AP

Chinese hackers broke into the computer networks housing the personal information of all federal US government employees in March in an apparent attempt to target people who had applied for top-secret security clearances.

News of the breach, first reported by The New York Times, came as US secretary of state John Kerry is visiting Beijing for an annual summit on Sino-American relations. Kerry's visit was already happening at a time of tense relations between China and the US over cyber security. Documents obtained by National Security Agency (NSA) whistleblower Edward Snowden showed the US has targeted China's political leaders, military and Huawei, a major maker of computer network equipment.

Speaking at a news conference in Beijing Thursday, Kerry said of the breach, "At this point in time, it does not appear to have compromised any sensitive material." But he also condemned

China’s cyber spying in unusually harsh language, saying it “harmed our business and threatened our nation's competitiveness."

Department of Homeland Security officials confirmed that they were aware of an attempt to hack into the Office of Personnel Management (OPM), which houses the personnel files of federal employees, including those applying for top-security clearance.

An official speaking on background said the attack was detected and blocked and that so far the government has not identified “any loss of personally identifiable information.” The US Computer Emergency Readiness Team (US-CERT), which is responsible for analysing and reducing cyber threats, continues to investigate the incident.

The attack appears to have targeted a system called e-QIP, in which federal employees applying for security clearances enter personal information, including previous jobs, foreign contacts and personal information like financial information and past drug use. Federal employees with security clearances are often required to update their personal information through the website.

The discussions between Kerry and his Chinese counterparts were already likely to be complicated this year both by Snowden’s revelations and by the Justice Department’s decision in May to indict five members of the People’s Liberation Army (PLA) on charges that they hacked into the systems of top US nuclear plant and solar power and steel firms in order to steal trade secrets, the first time the US has brought such criminal charges against a foreign country.

The charges outlined the hacking of five US companies and a trade union, including US Steel, the country’s largest steelmaker, by agents of the PLA’s Unit 61398, regarded by experts as one of the most prolific hacking organizations targeting Western companies.

The charges were largely symbolic, China has no extradition treaty with the US, and Beijing reacted by suspending cyber talks that had been initiated with the US.

http://www.theguardian.com/world/2014/jul/10/china-hackers-us-government-employee-database/print