+--
--------+

Obama Invokes Cold-War Law to Unmask Chinese Telecom Spyware (1) 2011-11-30 19:45:44.482 GMT

(Updates with month of survey in second paragraph.)

By Michael Riley

Dec. 1 (Bloomberg) -- The U.S. is invoking Cold War-era national-security powers to force telecommunication companies including AT&T Inc. and Verizon Communications Inc. to divulge confidential information about their networks in a hunt for Chinese cyber-spying.

In a survey distributed in April, the U.S. Commerce Department asked for a detailed accounting of foreign-made hardware and software on the companies' networks. It also asked about security-related incidents such as the discovery of "unauthorized electronic hardware" or suspicious equipment that can duplicate or redirect data, according to a copy of the survey reviewed by Bloomberg News.

The survey represents "very high-level" concern that China and other countries may be using their growing export sectors to develop built-in spying capabilities in U.S.
networks, said a senior U.S. intelligence official who asked not to be named because he wasn't authorized to speak on the matter.

"This is beyond vague suspicions," said Richard Falkenrath, a senior fellow in the Council on Foreign Relations Cyberconflict and Cybersecurity Initiative. "Congress is now looking at this as well, and they're doing so based on very specific material provided them in a classified setting" by the National Security Agency, he said.

Dozens of Companies

The survey went to dozens of telecommunications companies, software makers and information-security companies, including some foreign firms, according to James Lewis, a cyber-security expert at the Center for Strategic and International Studies, or CSIS, in Washington. Lewis said AT&T and Verizon Communications were among the companies that received it.

Several of the companies were hesitant to cooperate because they had learned the Commerce Department unit handling the survey had itself been hacked by the Chinese in 2006, creating the possibility that company data provided might become known to the Chinese, according to a former government official familiar with the discussions.

The Commerce Department refused a request by the companies for specific protocols to protect the data, according to the former official, who declined to be identified because the discussions were confidential.

Security Issues

Mark Siegel, a spokesman for Dallas-based AT&T, declined to comment on security issues. Edward McFadden, a spokesman for New York-based Verizon, said the company had received the survey and declined to

comment further. Eugene Cottilli, a Commerce Department spokesman in Washington, had no immediate comment on the survey.

So-called spyware implanted in hardware or hidden in millions of lines of code could intercept sensitive information while being almost impossible to detect, according to Joshua Pennell, president of IOActive Inc., a Seattle-based cyber security firm.

Spyware in critical U.S. networks that carry much of the country's data would make industrial espionage or the interception of politically sensitive information almost effortless. China now targets such information via focused cyber attacks, according to a November report by the Office of the National Counterintelligence Executive.

Detailed Outline

The survey required companies to provide a detailed outline of who made equipment including optical-transmission components, transceivers and base-station controllers. The results, which according to the survey were to be shared with the Defense Department, give U.S. authorities a map of who made which parts of the nation's networks, said Mischel Kwon, a former cyber- security official in President Barack Obama's administration.

Companies that refused to respond could face criminal penalties under the Defense Production Act, a 1950 law allowing the government to manage the wartime economy, according to the survey. The law was invoked sporadically during the Cold War, said Lewis, the computer security expert.

The possibility that foreign companies could be seeding equipment with "backdoors" to intercept data crossing U.S. networks could have implications for a global economy in which China plays a growing role as a component supplier.

"What we don't want to say is that we can't have technology coded or processed in another country," said Kwon, who has advised some of the companies sent the survey. "This is being read by some as very restrictive."

House Committee

Citing close links between China's military and the network equipment giant Huawei Technologies Co., the U.S. House Permanent Select Committee on Intelligence on Nov. 18 said it would investigate potential security threats posed by some foreign companies.

The committee's chairman, Representative Mike Rogers, a Michigan Republican, said China has increased cyber espionage in the U.S. He cited connections between Huawei's president, Ren Zhengfei, and the People's Liberation Army. Ren once worked as a military technologist.

"That's what we would call a clue," said Rogers, a former agent at the Federal Bureau of Investigation.

William Plummer, a spokesman for Shenzhen-based Huawei, said this month that the company welcomed an investigation.

"Huawei conducts its businesses according to normal business practices just like everybody in this industry," Plummer said this week in a phone interview. "Huawei is an independent company that is not directed, owned or influenced by any government, including the Chinese government."

Classified Information

The Obama administration has said little publicly about the matter, and much of the evidence fueling lawmakers' concerns remains classified.

The Commerce Department survey also illustrates the intelligence community's concern that manufacturers may insert spyware after equipment is installed, through either maintenance or automatic software updates. It asks companies to detail procedures they use to test software patches or updates to insure they are safe.

"It's the update function that is the core of the concern," said Lewis of the CSIS. "Huawei has offered to let people examine their source code to see if it is clean," he said. "Of course it's clean, but that's not the delivery vehicle, assuming there is one."

The survey also asks about incidents in which companies "detected undocumented functionality" in network hardware and software. The survey gave as examples the duplication and manipulation of data or redirection of transmissions.

Encrypted Data

Recipients were required to send an encrypted version of their responses by June 10 to the Commerce Department's Bureau of Industry and Security, according to the survey. That deadline was extended after companies expressed concern about how the data, much of which is proprietary, were to be handled, according to Portia Krebs, a spokeswoman for the U.S. Telecom Association, a Washington-based trade group.

U.S. Telecom and CTIA-The Wireless Association, another trade group, say the survey breaks with a tradition of voluntary cooperation between the industry and government over national security measures.

"We are deeply concerned by the lack of information regarding how this data is going to be used and shared," the groups said in a June 8 letter to then-Secretary of Commerce Gary Locke. "Our concerns are exacerbated by the fact that the department has chosen to direct the disclosure of this data pursuant to an assertion of authority under the Defense Production Act." Locke is now the U.S. ambassador to China.

Krebs and Amy Storey, a spokeswoman for the Washington- based CTIA, declined to comment further on the letter or their groups' concerns.

Picture Frame

In 2008, an Insignia brand digital picture frame was shipped with malicious software embedded during the manufacturing process. Best Buy Co., which makes Insignia products, traced the malware to a single computer at a contractor's plant in China, according to Carolyn Aberman, a company spokeswoman. Aberman declined to comment on whether the company discovered who may have planted it or why.

An analysis by Total Defense Inc., based in Islandia, New York, concluded the malware could have been a test run for a more sophisticated attack. It was designed to upload onto computers when the picture frame was connected to a computer and was capable of stealing large amounts of data while avoiding anti-virus detectors, the company's analysis found.

The malware came to light because the picture frame was a product that Richfield, Minnesota-based Best Buy, the world's biggest consumer-electronics retailer, pulled from the shelves.

Homeland Security

In July, Greg Schaffer of the Department of Homeland Security testified before the House Oversight and Government Reform Committee that the department knew of instances of foreign-made components seeded with cyber-spying technology. He declined to provide further details.

The Commerce Department survey also reflected U.S. intelligence community concerns over discounting and loan packages offered by foreign manufacturers.

It asks companies to list makers of telecommunications equipment that offer the steepest discounts. Other questions ask what information or other conditions manufacturers require in exchange for sales or leasing, including knowledge of physical access procedures for entering buildings.

Lewis of the CSIS said U.S. officials suspect the Chinese government is subsidizing the discounts to give U.S. companies incentives to buy Chinese-made network equipment.

“Huawei says they’re doing this and it’s completely legitimate, and it’s just us competing in the market,” Lewis said. “The other possibility is that they are doing it because they have an intelligence motive.”

For Related News and Information:
Legal headlines: TLAW <GO>
Bloomberg legal resources: BLAW <GO>
Telecommunication carriers: BI TELC <GO>

--Editors: Andrew Dunn, Mary Romano

To contact the reporter on this story:
Michael Riley in Washington at +1-202-624-1982 or
michaelriley@bloomberg.net.

To contact the editor responsible for this story:
Michael Hytha at +1-415-617-7137 or mhytha@bloomberg.net