Cybersecurity firm: Chinese hacking on US companies persists

October 19 2015, byKen Dilanian

In this Friday, Sept. 25, 2015, file photo, President Barack Obama, right, pauses during a joint news conference with Chinese President Xi Jinping in the Rose Garden of the White House in Washington. An analysis by a cybersecurity company finds that Chinese hacking attempts on American corporate intellectual property have occurred with regularity over the past three weeks. (AP Photo/Evan Vucci, File)

Chinese hacking attempts on American corporate intellectual property

have occurred with regularity over the past three weeks, suggesting that China almost immediately began violating its newly minted cyberagreement with the United States, according to a newly published analysis by a cybersecurity company with close ties to the U.S. government.

The Irvine, California-based company, CrowdStrike, says it documented seven Chinese cyberattacks against U.S. technology and pharmaceuticals companies "where the primary benefit of the intrusions seems clearly aligned to facilitate theft of intellectual property and trade secrets, rather than to conduct traditional national security-related intelligence collection."

"We've seen no change in behavior," said Dmitri Alperovich, a founder of CrowdStrike who wrote one of the first public accounts of commercial cyberespionage linked to China in 2011.

One attack came on Sept. 26, CrowdStrike says, the day after President Barack Obama and Chinese President Xi Jinping announced their deal in the White House Rose Garden. CrowdStrike, which employs former FBI and National Security Agency cyberexperts, did not name the corporate victims, citing client confidentiality. And the company says it detected and thwarted the attacks before any corporate secrets were stolen.

A senior Obama administration official, speaking on condition of anonymity because he was not allowed to discuss the matter publicly, said officials are aware of the report but would not comment on its conclusions. The official did not dispute them, however.

The U.S. will continue to directly raise concerns regarding cybersecurity with the Chinese, monitor the country's cyberactivities closely and press China to abide by all of its commitments, the official added.

The U.S.-China agreement forged last month does not prohibit cyberspying for national security purposes, but it bans economic espionage designed to steal trade secrets for the benefit of competitors. That is something the U.S. says it doesn't do, but Western intelligence agencies have documented such attacks by China on a massive scale for years.

China denies engaging in such behavior, but threats of U.S. sanctions led Chinese officials to conduct a flurry of last-minute negotiations which led to the deal.

CrowdStrike on Monday released a timeline of recent intrusions linked to China that it says it documented against "commercial entities that fit squarely within the hacking prohibitions covered under the cyberagreement."

The intrusion attempts are continuing, the company says, "with many of the China-affiliated actors persistently attempting to regain access to victim networks even in the face of repeated failures."

CrowdStrike did not explain in detail how it attributes the intrusions to China, an omission that is likely to draw criticism, given the ability of hackers to disguise their origins. But the company has a long track record of gathering intelligence on Chinese hacking groups, and U.S. intelligence officials have often pointed to the company's work.

"We assess with a high degree of confidence that these intrusions were undertaken by a variety of different Chinese actors, including Deep Panda, which CrowdStrike has tracked for many years breaking into national security targets of strategic importance to China," Alperovich wrote in a blog posting that laid out his findings.

The hacking group known as Deep Panda, which has been linked to the

Chinese military, is believed by many researchers to have carried out the attack on insurer Anthem Health earlier this year.

CrowdStrike and other companies have tracked Deep Panda back to China based on the malware and techniques it uses, its working hours and other intelligence.

In 2013, another cybersecurity company, Mandiant, published a report exposing what it said was a hacking unit linked to China's People's Liberation Army, including identifying the building housing the unit in Beijing. Those findings were later validated by American intelligence officials.