The New York Times

May 19, 2013

Hackers From China Resume Attacks on U.S. Targets

By DAVID E. SANGER and NICOLE PERLROTH

WASHINGTON — Three months after hackers working for a cyberunit of China's People's Liberation Army went silent amid evidence that they had stolen data from scores of American companies and government agencies, they appear to have resumed their attacks using different techniques, according to computer industry security experts and American officials.

The Obama administration had bet that "naming and shaming" the groups, first in industry reports and then in the Pentagon's own detailed survey of Chinese military capabilities, might prompt China's new leadership to crack down on the military's highly organized team of hackers — or at least urge them to become more subtle.

But Unit 61398, whose well-guarded 12-story white headquarters on the edges of Shanghai became the symbol of Chinese cyberpower, is back in business, according to American officials and security companies.

It is not clear precisely who has been affected by the latest attacks. Mandiant, a private security company that helps companies and government agencies defend themselves from hackers, said the attacks had resumed but would not identify the targets, citing agreements with its clients. But it did say the victims were many of the same ones the unit had attacked before.

The hackers were behind scores of thefts of intellectual property and government documents over the past five years, according to a report by Mandiant in February that was confirmed by American officials. They have stolen product blueprints, manufacturing plans, clinical trial results, pricing documents, negotiation strategies and other proprietary information from more than 100 of Mandiant's clients, predominantly in the United States.

According to security experts, the cyberunit was responsible for a 2009 attack on the Coca-Cola Company that coincided with its failed attempt to acquire the China Huiyuan Juice Group. In 2011, it attacked RSA, a maker of data security products used by American government agencies and defense contractors, and used the information it collected from that attack to break into the computer systems of Lockheed Martin, the aerospace contractor.

More recently, security experts said, the group took aim at companies with access to the
September, it broke into the Canadian arm of Telvent, now Schneider Electric, which ke
more than half the oil and gas pipelines in North America.

Representatives of Coca-Cola and Schneider Electric did not return requests for commer
Lockheed Martin spokesman said the company declined to comment.

In interviews, Obama administration officials said they were not surprised by the resumption of the hacking

activity. One senior official said Friday that “this is something we are going to have to come back at time and again with the Chinese leadership,” who, he said, “have to be convinced there is a real cost to this kind of activity.”

Mandiant said that the Chinese hackers had stopped their attacks after they were exposed in February and removed their spying tools from the organizations they had infiltrated. But over the past two months, they have gradually begun attacking the same victims from new servers and have reinserted many of the tools that enable them to seek out data without detection. They are now operating at 60 percent to 70 percent of the level they were working at before, according to a study by Mandiant requested by The New York Times.

The Times hired Mandiant to investigate an attack that originated in China on its news operations last fall. Mandiant is not currently working for The New York Times Company.

Mandiant’s findings match those of Crowdstrike, another security company that has also been tracking the group. Adam Meyers, director of intelligence at Crowdstrike, said that apart from a few minor changes in tactics, it was “business as usual” for the Chinese hackers.

The subject of Chinese attacks is expected to be a central issue in an upcoming visit to China by President Obama’s national security adviser, Thomas Donilon, who has said that dealing with China’s actions in cyberspace is now moving to the center of the complex security and economic relationship between the two countries.

But hopes for progress on the issue are limited. When the Pentagon released its report this month officially identifying the Chinese military as the source of years of attacks, the Chinese Foreign Ministry denied the accusation, and People’s Daily, which reflects the views of the Communist Party, called the United States “the real ‘hacking empire,’ ” saying it “has continued to strengthen its network tools for political subversion against other countries.” Other Chinese organizations and scholars cited American and Israeli cyberattacks on Iran’s nuclear facilities as evidence of American hypocrisy.

At the White House, Caitlin Hayden, the spokeswoman for the National Security Council, said Sunday that “what we have been seeking from China is for it to investigate our concerns and to start a dialogue with us on cyberissues.” She noted that China “agreed last month to start a new working group,” and that the administration hoped to win “longer-term changes in China’s behavior, including by working together to establish norms against the theft of trade secrets and confidential business information.”

In a report to be issued Wednesday, a private task force led by Mr. Obama’s former director of national intelligence, Dennis C. Blair, and his former ambassador to China, Jon M. Huntsman Jr., lays out a series of proposed executive actions and Congressional legislation intended to raise the stakes for China.

“Jawboning alone won’t work,” Mr. Blair said Saturday. “Something has to change China’s calculus.”

The exposure of Unit 61398’s actions, which have long been well known to American intelligence agencies, did not accomplish that task.

One day after Mandiant and the United States government revealed the P.L.A. unit as the culprit behind hundreds of attacks on agencies and companies, the unit began a haphazard cleanup operation, Mandiant said.

Attack tools were unplugged from victims' systems. Command and control servers went silent. And of the 3,000 technical indicators Mandiant identified in its initial report, only a sliver kept operating. Some of the unit's most visible operatives, hackers with names like "DOTA," "SuperHard" and "UglyGorilla," disappeared, as cybersleuths scoured the Internet for clues to their real identities.

In the case of UglyGorilla, Web sleuths found digital evidence that linked him to a Chinese national named Wang Dong, who kept a blog about his experience as a P.L.A. hacker from 2006 to 2009, in which he lamented his low pay, long hours and instant ramen meals.

But in the weeks that followed, the group picked up where it had left off. From its Shanghai headquarters, the unit's hackers set up new beachheads from compromised computers all over the world, many of them small Internet service providers and mom-and-pop shops whose owners do not realize that by failing to rigorously apply software patches for known threats, they are enabling state-sponsored espionage.

"They dialed it back for a little while, though other groups that also wear uniforms didn't even bother to do that," Kevin Mandia, the chief executive of Mandiant, said in an interview on Friday. "I think you have to view this as the new normal."

The hackers now use the same malicious software they used to break into the same organizations in the past, only with minor modifications to the code.

While American officials and corporate executives say they are trying to persuade President Xi Jinping's government that a pattern of theft by the P.L.A. will damage China's growth prospects — and the willingness of companies to invest in China — their longer-term concern is that China may be trying to establish a new set of rules for Internet commerce, with more censorship and fewer penalties for the theft of intellectual property.

Eric Schmidt, the chairman of Google, said Friday that while there was evidence that inside China many citizens are using the Web to pressure the government to clean up industrial hazards or to complain about corruption, "so far there is no positive data on China's dealings with the rest of the world" on cyberissues.

Google largely pulled out of China after repeated attacks on its systems in 2009 and 2010, and now has its Chinese operations in Hong Kong. But it remains, Mr. Schmidt said, a constant target for Chinese cyberattackers.

David E. Sanger reported from Washington, and Nicole Perlroth from San Francisco.