PHYS.ORG

A few hacker teams do most China-based data theft

December 12 2011, By LOLITA BALDOR , Associated Press

As few as 12 different Chinese groups, largely backed or directed by the government there, commit the bulk of the China-based cyberattacks stealing critical data from U.S. companies and government agencies, according to U.S. cybersecurity analysts and experts.

The aggressive but stealthy attacks, which have stolen billions of dollars in intellectual property and data, often carry distinct signatures allowing U.S. officials to link them to certain hacker teams. Analysts say the U.S. often gives the attackers unique names or numbers, and at times can tell where the hackers are and even who they may be.

Sketched out by analysts who have worked with U.S. companies and the government on computer intrusions, the details illuminate recent claims by American intelligence officials about the escalating cyber threat emanating from China. And the widening expanse of targets, coupled with the expensive and sensitive technologies they are losing, is putting increased pressure on the U.S. to take a much harder stand against the communist giant.

It is largely impossible for the U.S. to prosecute hackers in China, since it requires reciprocal agreements between the two countries, and it is always difficult to provide ironclad proof that the hacking came from specific people.

Several analysts described the Chinese attacks, speaking on condition of anonymity because of the sensitivity of the investigations and to protect the privacy of clients. China has routinely rejected allegations of cyberspying and says it also is a target.

"Industry is already feeling that they are at war," said James Cartwright, a retired Marine general and former vice chairman of the Joint Chiefs of Staff.

A recognized expert on cyber issues, Cartwright has come out strongly in favor of increased U.S. efforts to hold China and other countries accountable for the cyberattacks that come from within their borders.

"Right now we have the worst of worlds," said Cartwright. "If you want to attack me you can do it all you want, because I can't do anything about it. It's risk-free, and you're willing to take almost any risk to come after me."

The U.S., he said, "needs to say, if you come after me, I'm going to find you, I'm going to do something about it. It will be proportional, but I'm going to do something ... and if you're hiding in a third country, I'm going to tell that country you're there. If they don't stop you from doing it, I'm going to come and get you."

Cyber experts say companies are frustrated that the government isn't doing enough to pressure China to stop the attacks or go after hackers in that country.

Much like during the Cold War with Russia, officials say the U.S. needs to make it clear that there will be repercussions for cyberattacks.

The government "needs to do more to increase the risk," said Jon Ramsey, head of the counter threat unit at the Atlanta-based Dell SecureWorks, a computer security consulting company. "In the private sector we're always on defense. We can't do something about it, but someone has to. There is no deterrent not to attack the U.S."

Cyberattacks originating in China have been a problem for years, but until a decade or so ago analysts said the probes focused mainly on the U.S. government - a generally acknowledged intelligence gathering activity similar to Americans and Russians spying on each other during the Cold War.

But in the last 10 to 15 years, the attacks have gradually broadened to target defense companies, then other critical industries, including energy and finance.

According to Ramsey and other cyber analysts, hackers in China have different digital fingerprints, often visible through the computer code they use, or the command and control computers that they use to move their malicious software.

U.S. government officials have been reluctant to tie the attacks directly back to the Chinese government, but analysts and officials quietly say they have tracked enough intrusions to specific locations to be confident they are linked to Beijing - either the government or the military. They add that they can sometimes glean who benefited from a particular stolen technology.

One of the analysts said investigations show that the dozen or so Chinese teams appear to get "taskings," or orders, to go after specific technologies or companies within a particular industry. At times, two or more of the teams appear to get the same shopping list and compete to be the first to get them or to pull off the greatest haul.

Analysts and U.S. officials agree that a majority of the cyberattacks seeking intellectual property or other sensitive or classified data are done by China-based hackers. Many of the cyberattacks stealing credit card or financial information come from Eastern Europe or Russia.

According to experts, the malicious software or high-tech tools used by the Chinese haven't gotten much more sophisticated in recent years. But the threat is persistent, often burying malware deep in computer networks so it can be used again and again over the course of several months or even years.

The tools include malware that can record keystrokes, steal and decrypt passwords, and copy and compress data so it can be transferred back to the attacker's computer. The malware can then delete itself or disappear until needed again.

Several specific attacks linked to China include:

- Two sophisticated attacks against Google's systems stole some of the Internet giant's intellectual property and broke into the Gmail accounts of several hundred people, including senior U.S. government officials, military personnel and political activists.

- Last year, computer security firm Mandiant reported that data was stolen from a Fortune 500 manufacturing company during business negotiations when the company was trying to buy a Chinese company.

- Earlier this year, McAfee traced an intrusion to an Internet protocol address in China and said intruders took data from global oil, energy and petrochemical companies.

A Chinese Foreign Ministry spokesman, Liu Weimin, did not respond Monday to the specific allegations about government-supported cyber-attacks but said Internet security is an issue the world needs to address collectively. The international community should "prevent the Internet from becoming a new battlefield," Liu said at a daily media briefing in

Beijing.

For the first time, U.S. intelligence officials called out China and Russia last month, saying they are systematically stealing American high-tech data for their own economic gain. The unusually forceful public report seemed to signal a new, more vocal U.S. government campaign against the cyberattacks.

The next step, said Cartwright, must be a full-throated U.S. policy that makes it clear how the U.S. will deal with cyberattacks, including the attackers as well as the nations the attacks are routed through. Once an attack is detected, he said, the U.S. should first go through the State Department to ask the country to stop the attack. If the country refuses, he said, the U.S. will have the right to stop the computer server from sending the attack by whatever means possible while still avoiding any collateral damage.

Citation: A few hacker teams do most China-based data theft (2011, December 12) retrieved 27 April 2024 from https://phys.org/news/2011-12-hacker-teams-china-based-theft.html