Chinese military hackers target space industry

June 10 2014

Pedestrians walk past the skyline of the city's financial district in Shanghai on October 8, 2010

A Chinese military unit has run a hacking campaign that includes sending bogus email in a bid to intercept Western satellite communications and aerospace secrets, a US security firm said.

The report by the California-based firm Crowdstrike points to broader

hacking by China weeks after the United States for the first time filed charges against Chinese military officers over alleged cyber-espionage.

Dubbed "Putter Panda" for its focus on the golf-playing set, the Shanghai-based unit is a "determined adversary group" that has operated since at least 2007 by sending email attacks that target Microsoft Outlook, Adobe Reader and other common software, Crowdstrike said.

Putter Panda's strategy includes sending email from innocuous-looking addresses—mike.johnson_mj@yahoo.com was one example—and offering fake invitations in hopes that users will click and unwittingly give hackers access to their computer systems.

One attachment sent to workers at the Toulouse Space Center in France was a false brochure for a local yoga studio, promoting "a universal method to better know yourself, the universe and the gods, as recommended by Socrates."

Crowdstrike, in the report released Monday, said that Putter Panda appears bent on "obtaining intellectual property and industrial secrets related to defense technology" with an intent to "conduct space surveillance, remote sensing and interception of satellite communications."

Putter Panda "is likely to continue to aggressively target Western entities that hold valuable information or intellectual property relevant to these interests," it said.

Crowdstrike linked email addresses associated with Putter Panda to a personal blog of a 35-year-old named Chen Ping. On the blog, he said he works for the "military/police" and posted pictures that appear to show him exercising in front of soldiers and wearing army-style khaki as he drunkenly celebrated a birthday.

Crowdstrike linked Putter Panda with the People's Liberation Army's Unit 61486 in a high-rise building in Shanghai's northern Zhabei district.

The group is in addition to the already-known Unit 61398. A report last year by another security firm, Mandiant, said that Unit 61398 employed thousands of workers in a 12-story building near Shanghai who pilfered intellectual property and government secrets overseas.

A US grand jury last month indicted five officers from Unit 61398 for allegedly breaking into US computers to benefit Chinese state-owned companies, leading to US job losses in the steel, solar and other industries.

China summoned the US ambassador to protest and suspended cooperation on cyber issues. China accused the United States of hypocrisy as Washington conducts sweeping surveillance around the world, as revealed by former contractor Edward Snowden.

© 2014 AFP