China's PLA controls hackers: US IT security firm

February 19 2013, by Veronika Oleksyn

China's army controls some of the most prolific hackers in the world, according to a new report Tuesday by an Internet security firm that traced a host of cyberattacks to an anonymous building in Shanghai.

China's army controls hundreds if not thousands of virulent and cutting-edge hackers, according to a report Tuesday by a US Internet security firm that traced a host of cyberattacks to an anonymous building in Shanghai.

Mandiant said its hundreds of investigations showed that groups hacking into US newspapers, government agencies, and companies "are based primarily in China and that the Chinese government is aware of them".

The 74-page report focused on one group, which it called "APT1" from the initials "Advanced Persistent Threat". The New York Times, citing experts, said the group was targeting crucial infrastructure such as the US energy grid.

"We believe that APT1 is able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support," Mandiant said.

The group, it said, was believed to be a branch of the People's Liberation Army called Unit 61398, and digital signatures from its cyberattacks were traced back to the direct vicinity of a nondescript, 12-story building on the outskirts of Shanghai.

"We believe the totality of the evidence we provide in this document bolsters the claim that APT1 is Unit 61398," it said, estimating it is "staffed by hundreds, and perhaps thousands of people".

China's defence ministry said its army had never supported any kind of hacking activity.

"Not only are reports that China's army has been involved in hacking unprofessional, they do not fit with the facts," the ministry said in a statement to AFP.

"Hacking attacks are a global problem. Like other countries, China also faces the threat of hacking attacks, and is one of the main countries falling victim to hacking attacks."

The country's foreign ministry rejected "groundless accusations" of Chinese involvement in hacking and said China was itself a major victim, with most overseas cyberattacks against it originating in the US.

A series of brazen IT attacks on America's most high-profile media outlets, reported by The New York Times and the Wall Street Journal, as well as on Twitter and others, have revived concerns over Chinese hackers.

The Times said hackers stole corporate passwords and accessed the personal computers of 53 employees after the newspaper published a report on the family fortune of China's Premier Wen Jiabao.

Clients including The Times have hired Mandiant to clean up their systems after cyberattacks.

In its report, Mandiant alleged that APT1—known also as "Comment Crew" for its practice of planting viruses on the comment sections of websites—has stolen hundreds of terabytes of data from at least 141 organisations spanning 20 industries.

The Times, which was given early access to the report, said the researchers had found that the Comment Crew was increasingly focused on companies involved in US infrastructure, including in its electrical power grid, gas lines and water works.

One target, the newspaper reported, was a company with remote access to more than 60 percent of oil and gas pipelines in North America.

In his recent State of the Union address, US President Barack Obama said the potential ability of outsiders to manipulate critical US infrastructure was a major concern.

"We know foreign countries and companies swipe our corporate secrets," Obama said.

"Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air-traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."

The building pinpointed as the hacking HQ sits in Shanghai's northern suburb of Gaoqiao, near a petrochemical complex and surrounded by small shops.

There is no name plate outside, but framed posters showing soldiers are displayed on a high wall surrounding the complex, while the Chinese PLA's symbol of a red star is mounted over the main door of the building.

One soldier in camouflage uniform stood at the main gate Tuesday, an AFP correspondent saw. Another wearing a PLA overcoat was stationed in the guard house, close to a sign reading "No photography" in both English and Chinese.