Chinese hackers seen as increasingly professional (Update)

February 25 2013, by Christopher Bodeen

In this Feb. 20, 2013 photo, the building housing "Unit 61398" of the People's Liberation Army is seen in the outskirts of Shanghai. For state-backed cyberspies such as the Chinese military unit implicated by a U.S. security firm in a computer crime wave, hacking foreign companies can produce high-value secrets ranging from details on oil fields to advanced manufacturing technology. This week's report by Mandiant Inc. adds to mounting suspicion that Chinese military experts are helping state industry by stealing secrets from Western companies possibly worth hundreds of millions of dollars. The Chinese military

has denied involvement in the attacks. (AP Photo/Kyodo News)

Beijing hotly denies accusations of official involvement in massive cyberattacks against foreign targets, insinuating such activity is the work of rogues. But at least one piece of evidence cited by experts points to professional cyberspies: China's hackers don't work weekends.

Accusations of state-sanctioned hacking took center stage this past week following a detailed report by a U.S.-based Internet security firm Mandiant. It added to growing suspicions that the Chinese military is not only stealing national defense secrets and harassing dissidents but also pilfering information from foreign companies that could be worth millions or even billions of dollars.

Experts say Chinese hacking attacks are characterized not only by their brazenness, but by their persistence.

"China conducts at least an order of magnitude more than the next country," said Martin Libicki, a specialist on cyber warfare at the Rand Corporation, based in Santa Monica, California. The fact that hackers take weekends off suggests they are paid, and that would belie "the notion that the hackers are private," he said.

Libicki and other cyber warfare experts have long noted a Monday-through-Friday pattern in the intensity of attacks believed to come from Chinese sources, though there has been little evidence released publicly directly linking the Chinese military to the attacks.

Mandiant went a step further in its report Tuesday saying that it had traced hacking activities against 141 foreign entities in the U.S. Canada, Britain and elsewhere to a group of operators known as the "Comment

Crew" or "APT1," for "Advanced Persistent Threat 1," which it traced back to the People's Liberation Army Unit 61398. The unit is headquartered in a nondescript 12-story building inside a military compound in a crowded suburb of China's financial hub of Shanghai.

Attackers stole information about pricing, contract negotiations, manufacturing, product testing and corporate acquisitions, the company said.

Hacker teams regularly began work, for the most part, at 8 a.m. Beijing time. Usually they continued for a standard work day, but sometimes the hacking persisted until midnight. Occasionally, the attacks stopped for two-week periods, Mandiant said, though the reason was not clear.

China denies any official involvement, calling such accusations "groundless" and insisting that Beijing is itself a major victim of hacking attacks, the largest number of which originate in the U.S. While not denying hacking attacks originated in China, Foreign Ministry spokesman Hong Lei said Thursday that it was flat out wrong to accuse the Chinese government or military of being behind them.

Mandiant and other experts believe Unit 61398 to be a branch of the PLA General Staff's Third Department responsible for collection and analysis of electronic signals such as e-mails and phone calls. It and the Fourth Department, responsible for electronic warfare, are believed to be the PLA units mainly responsible for infiltrating and manipulating computer networks.

China acknowledges pursuing these strategies as a key to delivering an initial blow to an opponent's communications and other infrastructure during wartime—but the techniques are often the same as those used to steal information for commercial use.

China has consistently denied state-sponsored hacking, but experts say the office hours that the cyberspies keep point to a professional army rather than mere hobbyists or so-called "hacktivists" inspired by patriotic passions.

Mandiant noticed that pattern while monitoring attacks on the New York Times last year blamed on another Chinese hacking group it labeled APT12. Hacker activity began at around 8:00 a.m. Beijing time and usually lasted through a standard workday.

The Rand Corporation's Libicki said he wasn't aware of any comprehensive studies, but that in such cases, most activity between malware embedded in a compromised system and the malware's controllers takes place during business hours in Beijing's time zone.

Richard Forno, director of the University of Maryland Baltimore County's graduate cybersecurity program, and David Clemente, a cybersecurity expert with independent analysis center Chatham House in London, said that observation has been widely noted among cybersecurity specialists.

"It would reflect the idea that this is becoming a more routine activity and that they are quite methodical," Clemente said.

The PLA's Third Department is brimming with resources, according to studies commissioned by the U.S. government, with 12 operation bureaus, three research institutes, and an estimated 13,000 linguists, technicians and researchers on staff. It's further reinforced by technical teams from China's seven military regions spread across the country, and by the military's vast academic resources, especially the PLA University of Information Engineering and the Academy of Military Sciences.

The PLA is believed to have made cyber warfare a key priority in its war-

fighting capabilities more than a decade ago. Among the few public announcements of its development came in a May 25, 2011 news conference by Defense Ministry spokesman Geng Yansheng, in which he spoke of developing China's "online" army.

"Currently, China's network protection is comparatively weak," Geng told reporters, adding that enhancing information technology and "strengthening network security protection are important components of military training for an army."

Unit 61398 is considered just one of many such units under the Third Department responsible for hacking, according to experts.

Greg Walton, a cyber-security researcher who has tracked Chinese hacking campaigns, said he's observed the "Comment Crew" at work, but cites as equally active another Third Department unit operating out of the southwestern city of Chengdu. It is tasked with stealing secrets from Indian government security agencies and think tanks, together with the India-based Tibetan Government in Exile, Walton said.

Another hacking outfit believed by some to have PLA links, the "Elderwood Group," has targeted defense contractors, human rights groups, non-governmental organizations, and service providers, according to computer security company Symantec.

It's believed to have compromised Amnesty International's Hong Kong website in May 2012, although other attacks have gone after targets as diverse as the Council on Foreign Relations and Capstone Turbine Corporation, which makes gas microturbines for power plants.

Civilian departments believed to be involved in hacking include those under the Ministry of Public Security, which commands the police, and the Ministry of State Security, one of the leading clandestine intelligence

agencies. The MSS is especially suspected in attacks on foreign academics studying Chinese social issues and unrest in the western regions of Tibet and Xinjiang.

Below them on the hacking hierarchy are private actors, including civilian universities and research institutes, state industries in key sectors such as information technology and resources, and college students and other individuals acting alone or in groups, according to analysts, University of Maryland's Forno said.

China's government isn't alone in being accused of cyber espionage, but observers say it has outpaced its rivals in using military assets to steal commercial secrets.

"Stealing secrets is stealing secrets regardless of the medium," Forno said. "The key difference is that you can't easily arrest such electronic thieves since they're most likely not even in the country, which differs from how the game was played during the Cold War."