Internet sleuths add evidence to chinese military hacking accusations
Nicole Perlroth

Regular users of the Internet have been busy in the week since The New York Times reported that Mandiant, a computer security firm, had tied a prolific Chinese hacking group to a specific People's Liberation Army unit in Shanghai.

Chinese-speaking users and amateur hackers have scoured the Internet for traces of the online personas of those who Mandiant claims work on behalf of China's P.L.A. Unit 61398. The new evidence, while circumstantial, adds to the signs suggesting Chinese military efforts to hack into American corporate computer systems. Mandiant said that in one case, people were able to trace one of the P.L.A.'s hackers to an apartment building located 600 meters from the military unit's headquarters. In another, they were able to trace one hacker back to the P.L.A.'s Information Engineering University, described by American computer security researchers as one of the Chinese military's top training schools for computer hacking. They also found recruitment notices for Unit 61398, suggesting the group has been active since at least 2004, despite the fact that the unit's headquarters were not built until later.

In its report, Mandiant singled out a hacker named "DOTA," possibly shorthand for the video game "Defense of the Ancients," which is often abbreviated to DotA. That hacker created e-mail accounts that were used to begin several cyberattacks. The password for several of those accounts were a play on the Chinese military unit's designation. To register the accounts, DOTA used a Shanghai phone number.

This past week, Chinese-speaking Internet users disclosed on Twitter that DOTA's telephone number was listed in a 2009 ad for a Shanghai apartment rental. The apartment is 600 meters from Unit 61398's headquarters.

Another online persona that Mandiant singled out was of a military hacker named "Superhard." The author of a cybercrime blog, Cyb3rsleuth, connected the user name "Superhard_M" to the e-mail address mei_qiang_82@hotmail.com. That e-mail address was also used in a job posting, in which the person lists his skills and interests as "network security and developing hacking tools." The address listed in the post matched the address for the Information Engineering University. In a Northrop Grumman report for the U.S.-China Economy and Security Review Commission last year, defense analysts said the school, in Zhengzhou, Henan Province, "is perhaps the military university with the most comprehensive involvement in information warfare and computer network operations training, planning and possibly also execution."

Cyb3rsleuth found that a P.L.A. university student named Mei Qiang was co-author of two papers about hacking in 2007 and 2008, one titled "HTTP Session Hijacking on Switch LAN and Its Countermeasures" and the other "Stack Protection Mechanisms in Windows Vista."

Mandiant's report found that Unit 61398's headquarters in the Pudong new area of Shanghai was not built until early 2007. But China Digital Timesfound a 2004 military recruitment notice on a Zhejiang University Web site: "Unit 61398 of China's People's Liberation Army (located in Pudong District, Shanghai) seeks to recruit 2003-class computer science graduate students."

"This corroborates our assertions concerning the kinds of personnel that Unit 61398 recruits," Mandiant said in a blog post online. "This also indicates Unit 61398 has been operating in Pudong since 2004, even though the current headquarters facility was not built and operational until years later."

Fonte: The New York Times, New York, 27 Feb. 2013, International.