Issue: Cybersecurity

Short Article: China's Unit 61398 Pulled From the Shadows

By: Pat Wechsler

Pub. Date: February 1, 2016
Access Date: March 8, 2024
DOI: 10.1177/237455680203.n6
Source URL: https://businessresearcher.sagepub.com/sbr-1775-98146-2715481/20160201/short-article-chinas-unit-61398-pulled-from-the-shadows

State seeks to gain economic advantage from hacking

Executive Summary

Chinese hackers have become a state-controlled tool in world trade, stealing information from governments and companies in order to better their nation's competitive position, according to cybersecurity experts. They employ a strategy known as “advanced persistent threat,” or APT, to siphon data over extended periods.

Full Article

In May 2014, federal prosecutors charged five men in data breaches at several large U.S. companies, including Westinghouse, U.S. Steel and Alcoa. [1] Online, the accused went by such names as KandyGoo, UglyGorilla and WinXYHappy, the criminal complaint said. But what made these defendants particularly noteworthy was their employer: They all were—and presumably still are—officers in the People's Liberation Army (PLA) of China.

According to the Justice Department, the five worked for a PLA division known as Unit 61398, a storied computer hacking center believed to house some of China's most proficient and prolific state-sponsored cyberspies. [2] In a 31-count indictment, the government accused the men of stealing trade secrets and other sensitive, internal communications and data from the companies to benefit Chinese manufacturers, including state-owned enterprises.

“Success in the global marketplace should be based solely on a company's ability to innovate and compete, not on a sponsor government's ability to spy and steal business secrets,” U.S. Attorney General Eric Holder said when he announced the indictments. [3] “This administration will not tolerate actions by a nation that seeks to illegally sabotage American companies and undermine the integrity of fair competition in the operation of the free market.”

While the United States and other major world powers spy on each other by whatever means necessary—including hacking—Unit 61398 and more than 20 other state-controlled operations in China take cyberspying one step further, according to the U.S. government and many cybersecurity experts. They use hacking as an economic tool of global trade, usurping intellectual property and competitive strategies from companies worldwide in an effort to provide their domestic industries with an economic advantage over their rivals.

Before the indictments, Unit 61398 already was well known in cyber circles, thanks in part to an exhaustive February 2013 report by computer consultant Mandiant. [4] Now a subsidiary of network security company FireEye, Mandiant had tracked the shadowy Chinese hacker group since 2004 in an effort to unlock the secrets of its network attack strategy—a variation on the increasingly popular “advanced persistent threat” approach to hacking, or APT. When hackers employ APT, their goal is to gain access to a corporate or governmental computer network and remain there under the radar for weeks, months, even years. All the while, they are gathering and ultimately extracting as much data as possible before leaving. [5] Mandiant designated this particular Chinese hacking team APT1.

Operating primarily out of a nondescript 12-story white tower off Datong Road in the Pudong New Area of Shanghai, APT 1 represents one group of actors in a “long-running and extensive cyber espionage campaign” that Mandiant contended could only be sustained with “direct government support.” Based on the size of APT1's facility, Mandiant speculated that APT1 employs hundreds and possibly as many as 2,000 people.

Since 2006, APT1 has stolen hundreds of terabytes of data, including valuable intellectual property, from more than 140 organizations and companies, according to Mandiant. Often striking dozens of enterprises simultaneously, APT1 targets industries identified as strategic for China's growth. Close to 90 percent of targets were based in nations where English was the primary language.

“The activity we have directly observed likely represents only a small fraction of [the unit's] cyber espionage,” Mandiant concluded in the report. While Mandiant could not definitively say that APT1 and Unit 61398 were one and the same, the consulting firm left little doubt that the evidence supported such a conclusion.

“In seeking to identify the organization behind this activity, our research found that People's Liberation Army (PLA's) Unit 61398 is similar to APT1 in its mission, capabilities, and resources,” the Mandiant report stated. “PLA Unit 61398 is also located in precisely the same area from which APT1 activity appears to originate.”

APT1 has a well-defined attack methodology, according to Mandiant, inhabiting the networks of victims for an average of 356 days and even remaining in one undetected for an astounding 1,764 days—just short of five years. At opportune moments, the hacking team would steal intellectual property, including technology designs and proprietary processes, and then crawl back into the digital shadows.

Even before the Mandiant profile, the U.S. government and computer security experts had studied Unit 61398 for years but under various code names, including “Comment Crew,” “Shanghai Group” and “Byzantine Candor”—a designation used by U.S. intelligence agencies

until WikiLeaks made public its significance. [6] One signature infiltration strategy of the unit has been to enter computer systems through the comment sections of websites or social media—hence the name Comment Crew. After the Mandiant report, Unit 61398 went dark for a time, only to emerge several months later with a few new techniques and new malware. [7]

So how effective was the U.S. strategy of indictments at deterring Chinese cybertheft? "I thought it was tremendously effective, in that it irritated the heck out of the Chinese," James Lewis, a cybersecurity expert at the Center for Strategic and International Studies, told Foreign Policy, more than a year after the criminal complaint was brought. [8]

But Lewis admitted there was no evidence that the indictments prompted China to alter its behavior. As they did after the Mandiant report, Chinese hackers simply changed their malware and infrastructure of choice. Instead of Unit 61398, the prominent player in more recent hacks reportedly was an APT known as "Deep Panda," a Chinese cyber unit, also believed to be affiliated with the Chinese army. The unit has been implicated in the theft of nearly 80 million records from health insurer Anthem and 11 million from Blue Cross Blue Shield carrier Premera. [9]

In December 2015, the Chinese government took the unprecedented step of arresting several people alleged to have taken part in the APT directed against the U.S. Office of Personnel Management. [10] During that network penetration, which was active from the spring of 2014 until the spring of 2015, as many as 22 million files of current and former government employees were compromised, including sensitive information collected in connection with background checks for classified postings, and even fingerprints. Cyber experts had tracked the hackers back to China, and U.S. officials threatened economic sanctions unless the Chinese took action.

The identities of the hacking suspects have not been made public, and U.S. officials are not yet sure whether those arrested were actually the perpetrators. The Washington Post reported that U.S. government officials believed that the hackers behind the OPM breach may work for the Ministry of State Security or act as contractors for the agency. [11]

For now, the Chinese appear to want to play nice on cybersecurity. Besides the arrests, President Xi Jinping concluded a cybersecurity agreement with President Obama that calls on both governments to refrain from computer-enabled theft of intellectual property. [12]

Some analysts see the agreement as a good start. Skeptics, however, point to that nondescript 12-story white tower off Datong Road in Shanghai to question China's intentions. Chasing down Chinese hackers, they warn, remains a Sisyphean pursuit.

About the Author

Pat Wechsler is a veteran journalist who has held senior editing and writing positions at Business Week, Bloomberg, Newsday and New York magazine. Most recently, she served as a senior vice president at FleishmanHillard, where she created and ran an award-winning online thought-leadership magazine focused on the intersection of communications, marketing and media.

Notes

[1] United States of America v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, Criminal No. 14-118, U.S. District Court, Western District of Pennsylvania, May 1, 2014, http://tinyurl.com/zcuzpl9.

[2] "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," news release, Office of Public Affairs, Department of Justice, May 19, 2014, http://tinyurl.com/lk9mjoj.

[3] Ibid.

[4] David E. Sanger, David Barboza and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," The New York Times, Feb. 18, 2013, http://tinyurl.com/hp69kxo.

[5] "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, February 2013, http://tinyurl.com/bjnsvjo.

[6] Sanger, Barboza and Perlroth, op. cit.

[7] Jeremy Kirk, " 'Comment Crew' hackers resurface, security firm reports," PC World, June 29, 2013, http://tinyurl.com/qzlp5u8.

[8] Elias Groll, "The U.S. Hoped Indicting 5 Chinese Hackers Would Deter Beijing's Cyberwarriors. It Hasn't Worked," Foreign Policy, Sept. 2, 2015, http://tinyurl.com/jotp2gz.

[9] Jeremy Kirk, "Premera, Anthem data breaches linked by similar hacking tactics," PCWorld, March 17, 2015, http://tinyurl.com/jgkzxm6.

[10] Ellen Nakashima, "Chinese government has arrested hackers it says breached OPM database," The Washington Post, Dec. 2, 2015, http://tinyurl.com/hjluugw.

[11] Ibid.

[12] Julie Hirschfeld Davis and David E. Sanger, “Obama and Xi Jinping of China Agree to Steps on Cybertheft,” The New York Times, Sept. 25, 2015, http://tinyurl.com/ngrqx9w.