Sino-Cyber Espionage: An Overview of the Strategies of Units 61398 and 61486 in the People's Liberation Army of China

James A. King

University of North Georgia

ABSTRACT

This paper begins with an overview of the two most notorious hacking divisions of the People's Liberation Army. It draws from several different articles concerning the state of the internet from *Congress, CrowdStrike, Verizon,* and *Akamai* as well as reports from the United States Department of Justice. The scope of this paper is limited because of the level of security clearance needed to access the real information on the exploits of the Chinese in the corporate sector, but the ramifications of said exploits are clear. The discussion provides examples from the Department of Justice on what the Chinese have done to American companies and some of the strategies that they have used. It also expounds on some of the repercussions of the strategies on the markets that were affected. Statistics are given from *The Economist* and *Wired* magazines that sourced the state of the internet reports from *Verizon* and *Akamai*. The recommendations are mainly ideas of International Relations to try to keep peace between the People's Republic of China and the United States of America. Extreme measures must, however, be considered if there are any more exploited vulnerabilities in the federal sector. This paper mainly serves to inform the reader of the attacks that the Chinese use, who they target and why, and possible solutions to the problem of cyber corporate espionage.

INTRODUCTION

Life as we know it would not exist without the internet. This paper is an in-depth analysis of how cyber-crime affects those who access the internet in the United States of America with a special interest in the Chinese involvement in impeding, disturbing, and profiting from that access. The People's Liberation Army has developed several intricate and sophisticated cyber-warfare divisions based in Shanghai. The main two divisions are PLA Units 61398 and 61486. These may seem like just another label for some part of the Chinese intelligence, dissociated from any notoriety by the simplicity of their nomenclature, but these units are some of the most world-renowned hacking teams to ever be conceived by any government. They are likely responsible in the recent hacks of the United States Post Office, Office of Personnel Management, and Internal Revenue Service in the federal sector. Some of their leadership are on the most wanted list, or the United States has asked for them to be brought to trial in America for corporate espionage for what they have done to the US Steel Corporation, Westinghouse Electric, SolarWorld, and other companies in the private sector (Justice 2014).

This paper is limited in the facts that it contains about the People's Liberation Army because most of the information on the subject of corporate and federal hacking for government entities is classified by the United States government. Sources from briefings to Congress, CrowdStrike, Verizon, and Akamai to give some relative credibility to the facts and speculations contained in the discussion. This paper is able to determine some of the attacks used by the Chinese, such as spear-phishing, which appears to be their most used, but most of the specifics of how the People's Liberation Army infiltrates networks is also classified. The main purpose of the paper is to give an overview of the exploits of Chinese nationals in America and the impact it has had on the cyber community and our government.

PLA Unit 61486 is based in a militarized section of Shanghai. They are housed in a white office building that is deceptively ordinary. The only piece of evidence that cyber-warfare divisions are stationed inside are the military personnel scattered around the compound guarding access to these high-tech barracks. This unit is said to specialize in the reconnaissance of intelligence in the satellite industry based on the findings of military analysts at the Project 2049 institute in Arlington, Virginia. Targeting highly profitable aerospace engineering firms allows the Chinese limit funding in their space programs as a result of stealing sensitive ideas from the international private sector (Stokes 2012). Unit 61486 is documented using malware that comes in a PDF format, an invitation to aviation conferences to dupe whoever opens it into remote access to their network. They even used yoga brochures from Toulouse, France, a hub of aerospace engineering, to get into people's computers and networks. *CyberStrike*, an online security firm based out of California and founded by two executives of *McAfee*, estimate that the attacks could have affected hundreds if not thousands of computers (Sanger 2013). The PLA unit struck from international websites that were already compromised so that they could not be traced, but any

international site that goes through an *AT&T* database is almost guaranteed to be monitored by the National Security Administration of the United States of America. These are not as clean as the NSA attacks on foreign nations, which are routed through Germany or any other Western-European ally to remove traces of American involvement.

PLA Unit 61398 is housed in a militarized section of Shanghai on Datong Road and is circumscribed by normal first-world amenities such as massage parlors and restaurants (Sanger 2013). It is an inconspicuous spot for one of the most notorious hacking teams in the world. They are known for their zero-day attacks, reconstructing programs like Microsoft Word from the ground up to find vulnerabilities, and their prowess in different kinds of malware. Some of the most notorious confirmed attacks by unit 61398 are the attacks on the US Steel Corporation which gathered information on making cheap steal to destabilize the world's steel market and nearly drive the corporation out of business, the attack on Westinghouse Electric which is said to have stolen information on nuclear power, healthcare providers, and the attack on SolarWorld in the private sector (Justice 2014). In the federal sector the attacks have not been confirmed by the US government, but it is highly likely that the PLA had something to do with the breach at the Office of Personnel Management (where background checks are performed for application to the federal government and some twenty million identities compromised) the IRS, and the United States Post Office, in an effort to get the layout of what hacking and distributing social security numbers would be like. Unit 61398 has done the bulk of the hacking in the People's Liberation Army with five of its senior officials indicted already by the US for the US Steel, Westinghouse, and SolarWorld (Justice 2014).

DISCUSSION

It is hard to determine which act of "economic espionage" did the most damage. I became familiar with the attack on Westinghouse first because I was in the process of becoming a nuclear engineer at Georgia Tech and was keeping up with the latest news on the deal with the AP1000 reactors. This reactor design is one of the most cost effective to date, and is the design being used to build the new reactor at plant Vogel in Georgia. It is being built in China so that the Chinese can put what was supposed to be three online at the initial start of the deal, but what has grown to over twenty. As Westinghouse was negotiating the transfers for the technological systems needed to maintain this version of a nuclear reactor, one of the members of PLA unit 61398 was able to illegally acquire the documentation for different specifications on building the pipes, pipe supports, and pipe routing (Johnson 2014). This was very sensitive data valuable to Westinghouse. The unit did not stop there; it also illegally gathered the emails of the top decision makers in Westinghouse concerning the business venture between the company and the state owned enterprise of the People's Republic of China (Justice 2014). This all lead to the eventual indictment of senior official of unit 61398 Sun Kailiang by the United States of America.

In 2012, the Chinese decided to dump their solar panels into US markets, causing a detrimental rise in instability and prices to relatively hit rock bottom. The Chinese were selling their products at prices below what would be considered fair value, and this hit American solar panel companies very hard. At the same time it was uncovered that Wen Xinyu, a member of PLA unit 61398, had, with several co-conspirators, infiltrated SolarWorld's data systems and again stolen sensitive information (Justice 2014). This information not only concerned the manufacturing and painstaking research of the solar panels themselves, but the process of how the company managed cash flow, production line information, costs, and attorney-client communications regarding ongoing trade litigation (Justice 2014). This was an entirely new angle for Chinese intelligence to approach warfare and had not been seen, at least to the knowledge of the American public, before. This was a dirty war for money, but not just for profit. It was a war to destabilize a growing sector of the American economy in a time when we needed all of the growth that we could get.

The next private sector government hack that has been confirmed by the PLA unit 61398 is a combination of the previous two attacks' intentions. The Chinese stole trade secrets on manufacturing a product, like they did during the attack to secure engineering mechanisms for the AP1000 nuclear reactor, in order to destabilize a market, similar to what was done with the information from SolarWorld (Justice 2014). In terms of American jobs, the attack on the US Steel Corporation out of Pittsburgh, Pennsylvania was the worst of any of the attacks in the private sector. US Steel was trading with different Chinese steal companies including one state-owned company. According to the United States Department of Justice

(2014), Sun Kailiang sent a spear-phishing email to numerous members of US Steel's executives, targeting those who were setting up the preliminary litigation for the trade to happen with the Chinese state-owned company. The spear-phishing emails that were successful set up malware on numerous computers within the company, compromising their data's integrity and allowing unit 61398 to gather trade secrets from the top executives in the company. This compounded into an individual of 61398 gaining access to hostnames and the majority of devices on the US Steel network and eventually also gaining access to their vulnerable servers. The Chinese would not stop at just producing cheap steal and destabilizing yet another international market for the American manufacturers. PLA unit 61398 would eventually go for the jugular of trade between China and America by illegally accessing the strategies they would need to undermine before they were brought to the table by United States trade regulators (Johnson 2014).

Another member of unit 61398 used spear-phishing attacks on the company *Alcoa* (Justice 2014). *Alcoa* was set for a merger with a Chinese state owned company when the Chinese saw more fit to gain the upper hand yet again and make sure they were not making a mistake in 2008. The same member in 2012 gained access to "virtually every computer on the network" (Justice 2014) of the semiconductor company API while they were in the process of a joint venture with a Chinese state owned enterprise.

The Chinese used their unit 61398 in the People's Liberation Army to access the trade litigation strategies concerning their business with *US Steel*, *Westinghouse*, and a yet to be known amount of other companies (Justice 2014). The United States has only been able to confirm that these attacks happened during the trade deals between a Chinese state owned company and *Westinghouse* as well as the *United States Steel Corporation* and *SolarWorld*, but the future will only tell how many other companies the Chinese have infiltrated. To procure an advantage in trading with US Steel, unit 61398 hacked the United Steel Workers Union to see what strategies their head officials would use when making litigation against China to represent the workers of US Steel (Here's 2014). They also hacked US Steel's CEO John Surma and, in a separate instance, the CEO of Westinghouse. These are two of the most iconic American institutions. The aforementioned instances prove that no one can expect anything that they put online to be safe for long.

The statistics on the People's Liberation Army's internet intelligence exploits are astounding. According to an article by *The Economist* sourced in the *CrowdStrike* documentation led by the two executives from *McAfee* in southern California, there were more than seventy identified infiltrations, and even more unidentified in the corporate sector of America (Masters 2013). According to the source, once access was gained into a targeted computer, the hackers would stay inside of it for anywhere from five to

seven years, increasing their chances of getting caught while at the same time allowing for the slow trickle of vital information from corporate executives' networks.

In another article by *Wired* based in the United Kingdom, the *Akamai's* State of the Internet report was said to have announced that in the fourth quarter of 2012 China was responsible for forty one percent of all cyber-attacks in the world, which is more than all of the top ten below China's ranking combined (Reports 2013). Also in 2013, *Verizon's* Data Breach Investigation Report stated that in that year thirty percent of all cyber-attacks from around the world were based in China (Reports 2013). These are two enormous figures. In just one-fourth of one year, China was the source of more than the top ten other countries of the world's cyber escapades combined. Also in the next year, China's cyber exploits accounted for almost one third of the entire online community's crime and infiltration of networks.

Figure 1 (see Appendix A) is a bar graph of the different corporate sectors that the Chinese have infiltrated from 2006 to 2012. In one of the New York Times articles (Sanger 2013) it is proposed that PLA unit 61486 is responsible for the majority of the hacks in the second largest section of Figure 1, the aerospace industry. This is the only specific attribution that can be inferred from the sources because the Chinese have so many different units in the cyber division of the People's Liberation Army that every single attack could not possibly be unit 61398 (Stokes 2012). According to the graph there were roughly 80 major attacks that can be attributed to the Chinese during this time period, and most of the attacks happened in the information technology industry. The source of the figure did not state if the graph takes into consideration multiple attacks on the same company or just counts one attack per singular company.

RECOMMENDATIONS

One solution to the problem of corporate and federal cyber-attacks from the Chinese would be to stipulate that American-owned companies or companies or individuals with stock in American-owned companies cannot do business in any way, shape, or form with Chinese state owned enterprises. Every instance of a major attack in the corporate sector occurred when a company was dealing with a state owned enterprise of China. Eliminating the vulnerability of dealing with this sort of organization would eliminate having to deal with indicting Chinese nationals that are in the People's Liberation Army and ease tensions with the Chinese in that regard. Another way to solve the problem of state owned companies would be to tax American companies involved with Chinese state owned companies so heavily that they would have to weigh their potential profit margins internationally against this tax from the United States.

In order to actively defend, the Chinese term for their strategy in the South China Sea, against any unit of the People's Liberation Army's cyber division, America must implement a firewall just like China's. This firewall would not be to block, filter, and limit the American people's first amendment rights completely, but would filter international traffic and require permission, like a virtual passport, from the NSA to visit websites outside of the United States for the protection of our country's data integrity. These digital passports would be relatively easy to acquire and would generate considerable revenue from the private sector for the federal government. In addition to virtual passports for different country's domains, we would need to implement a spam filter for data coming from compromised international websites, similar to the ones unit 61398 uses to base their cyber-attacks from. We could attack the People's Republic of China to gain data on their current intentions to spread propaganda concerning what public relations battle they plan to wage, we could attack state owned enterprises, and we could shut off their internet like what was done to North Korea after the Sony incident, but these are extreme measures that would complicate our international relations to no end. China is just trying to wage economic warfare on the United States, not start a real war. Iranian and Russian nationals do the same thing in different and similar industries in order to gain information on business strategies as well as the international trade litigation techniques used by Americans. They are just trying to make a profit, not shed blood.

If, however, the attacks continue on the health care industry, on the United States Post Office, the Internal Revenue Service, and the Office of Personnel Management, our country must take drastic measures to defend the social security numbers of Americans so that the Chinese will not put them up for sale on the deep web. We must also consider the risk that identities will be compromised in the Central Intelligence Agency, Federal Bureau of Investigation, National Security Agency, Department of Homeland Security, and many other parts of the security forces of the United States government if we

allow these cyber-attacks to continue on the databases where we store the credentials for those that are part of our own espionage and security units. We cannot allow any unit of the People's Liberation Army to compromise identities, security credentials, social security numbers, or anything else that may be of value to the Chinese intelligence forces that are housed in a federal database.

REFERENCES

Foreign Spies Stealing US Economic Secrets In Cyberspace. (2011, October 1). Retrieved July 19, 2015, from http://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

Here's What Chinese Hackers Actually Stole From U.S. Companies. (2014, May 20). Retrieved July 19, 2015, from http://time.com/106319/heres-what-chinese-hackers-actually-stole-from-u-s-companies/

Johnson, K., & Leinw, D. (2014, May 19). U.S. accuses China of hacking Westinghouse, U.S. Steel. Retrieved July 19, 2015, from http://www.usatoday.com/story/news/nation/2014/05/19/us-accuses-china-of-cyber-espionage/9273019/

Justice News. (2014, October 8). Retrieved July 19, 2015, from http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

Masters of the cyber-universe. (2013, April 6). Retrieved July 19, 2015, from http://www.economist.com/news/special-report/21574636-chinas-state-sponsored-hackers-are-ubiquitousand-totally-unabashed-masters

Reports find China still largest source of hacking and cyber attacks (Wired UK). (2013, April 24). Retrieved July 19, 2015, from http://www.wired.co.uk/news/archive/2013-04/24/akamai-state-of-the-internet

Sanger, D., Barboza, D., & Perlroth, N. (2013, February 18). Chinese Army Unit Is Seen

Hacking Against U.S. Retrieved July 19, 2015, from http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all

Stokes. (2012, October 29). Countering Chinese Cyber Operations. Retrieved July 19, 2015, from http://project2049.net/documents/countering_chinese_cyber_operations_stokes_hsiao.pdf

APPENDIX A

Figure 1. Organizations Targeted by Chinese Hackers in the Private Sector (2013)