June 15, 2015

Jen Weedon

Manager, Threat Intelligence

FireEye, Inc.

Testimony before the U.S.-China Economic and Security Review Commission

Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China

Introduction

Thank you for the opportunity to testify. My name is Jen Weedon, and I am a Manager of Threat Intelligence at FireEye, Inc. FireEye provides software to stop today's advanced cyber threats, serving 3,100 customers in 67 countries. FireEye's Mandiant Consulting Services helps companies investigate and recover from intrusions and shore up their security programs.

Our Intelligence Team tracks the activities, tools, and targets of cyber threat actors globally, including groups we assess to be state-sponsored, financially motivated cyber criminals, or hacktivists. Much of the malicious activity that we see hitting our clients is from Advanced Persistent Threat (APT) groups. APT actors generally have some level of government sponsorship or support, persistently pursue their objectives, and are capable of using a full spectrum of tactics, techniques, and procedures ("TTPs) to conduct data theft and/or disrupt, deny, degrade, or destroy networks. One of our most publicized reports on an APT group was the APT1 report, which describes APT1's multi-year, enterprise-scale computer espionage campaign in detail and links APT1 to China's 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's 3rd Department (Unit 61398).

In our current environment, this type of state-sponsored cyber activity is a common tactic that nations use to gain advantage over one another. Well-resourced advanced cyber threats that use sophisticated TTPs are able to bypass conventional security deployments almost at-will. American companies are being forced to fight a battle against adversaries possessing nation-state capabilities, which is not a fair fight.

A successful cyber operation has the potential to significantly benefit a threat sponsor, and the magnitude of data theft we see is of virtually unquantifiable economic, political, and military value. Advanced cyber threats often emanate from countries that not only refuse to hold attackers accountable for their crimes but also provide resources and direction. Accordingly, there is very little risk and relatively few costs for them, given the enormous imbalance between the resources necessary to defend a network and the resources necessary to attack one. Cyberspace is an asymmetrical domain, where a single attacker can generate work for hundreds, if not thousands, of defenders.

Based on our threat intelligence work over the past 10 years, FireEye believes that the Chinese government largely uses cyber operations for three interrelated purposes: 1) to collect intelligence on other nations, 2) to conduct commercial espionage to enable and sustain economic growth, and 3) to maintain domestic control by strictly regulating and censoring the Internet. Out of the dozens of advanced cyber threat groups we track, the more than 20 China-based groups we watch are by far the most focused on commercial and political espionage.

Our experience and research has also revealed several key lessons:

First, nation state-backed groups are capable of circumventing even the best defenses, because they are well-resourced and relentless in pursuit of their goals.

Second, Chinese government-based cyber espionage groups continue to engage in wide-scale

commercial data theft at staggering rates, although their specific targets will likely evolve over time based on China's broader economic reorientation.

Third, not all Chinese threat groups that FireEye tracks are the same. They can have different government sponsors, different targets, and varying degrees of state-sponsorship or support. In addition, some threat actors and groups appear to be contractors. Certain groups and individuals moonlight on the side and conduct operations for financial gain. In spite of these differences, though, the vast majority of China-based advanced threat groups are engaged in massive theft of intellectual property from global corporations, particularly those involved in what the Chinese government views as areas of strategic importance.

Chinese Commercial Cyber Espionage Driven By National Priorities; Groups Relentless in their Pursuits

China's commercial cyber espionage activity likely supports Communist Party central planning policies designed to provide a competitive advantage for Chinese companies. This is a coordinated approach that pits government-backed Chinese enterprises against foreign firms in a race for innovation and economic dominance, often with detrimental effects for U.S. companies.[1]

The strategic importance of this economic espionage means that the actors are both well-resourced and relentless in their pursuit of a corporation's proprietary data. If one of these advanced threats targets a company, a security breach is inevitable. This even applies to companies with robust and mature cyber defenses. In 2014, FireEye conducted hundreds of investigations in 13 countries, and during these investigations, we found approximately 10 new pieces of malware per work-hour that had successfully bypassed the defenses of security-conscious organizations.

Chinese APT groups do not choose their commercial targets at random. FireEye's research and analysis indicates that there are probably both formal and informal tasking mechanisms between groups' sponsors and the actors conducting the intrusions.

China's Strategic Emerging Industries: A To-Do List for APT Groups

No sector has gone untouched by intrusions from China-based APT groups. In addition to the frequently publicized data theft from defense companies or government coffers, FireEye has also observed China-based APT groups targeting U.S. firms involved in strategic industries that are not as widely discussed. These industry sectors include electronics, telecommunications, robotics, data services, pharmaceuticals, mobile phone services, satellite communications and imagery, and business application software. In the past year, we have helped many organizations across a broad spectrum of sectors (e.g., business and professional services, finance, media and entertainment, healthcare, and construction and engineering) respond to Chinese APT intrusions.

Looking at the current active threats and corresponding data from over ten years of data collection, China-based APT groups consistently target future growth areas for both China and the U.S. These focus areas are described in China's Strategic Emerging Industries initiative, which is a component of the government's 12th Five-Year Plan.[2] The following table displays

China's Strategic Emerging Industries and the corresponding number of distinct threat groups we have seen targeting those sectors:

Strategic Emerging Industry (SEI)	No. of China-based APT Groups Targeting this SEI
Clean Energy Technology	3
Next-Generation IT	19
Biotechnology	6
High-End Equipment Manufacturing	22
Alternative Energy	7
New Materials	12
New Energy Vehicles	6

Figure 1: China-based APT groups' targeting of Strategic Emerging Industries

China's Economic Reorientation Will Inform its Future Commercial Cyber Espionage Strategy

China's nearly 20-year period of rapid economic growth has slowed following the global financial crisis, creating significant economic pressures. In response, China has prioritized rapid innovation and focused on stimulating domestic consumption, consumer spending, and services.[3] This reorientation will likely have a dramatic effect on the specific targets China pursues with its commercial cyber espionage program.

Chinese leadership will likely continue to use the theft of intellectual property through cyber means to acquire, mimic, and co-opt innovative foreign technologies. China's efforts to spur innovation will take on even greater urgency if the economy continues to slow and unemployment among college graduates continues to rise.[4] High rates of unemployment among the young and educated could be a destabilizing force in Chinese society, which is not something the Communist Party will tolerate.

Indeed, we're already seeing the targeting implications of China's desire for rapid innovation. This May, FireEye's Mandiant Consultant Services aided Penn State in an investigation of Chinese hackers who had been so deeply embedded in the computer network of its engineering college – which specializes in aerospace engineering, among other disciplines – that the network had to be taken offline.[5] Such an incident is unfortunately not the exception. In the past year alone, we responded to at least two other cyber espionage incidents involving top U.S. schools engaged in sensitive, state-of-the-art R&D.

APT actors will likely continue to target U.S. labs, university research institutions, and small businesses and start-ups – organizations that may lack either the understanding of the risk or the resources with which to secure their technical and scientific research. APT actors may also try to exploit trusted third-party relationships to compromise organizations with better defenses. Given

the Chinese leadership's focus on understanding and advancing entrepreneurship, actors may pursue information on the leadership, management, and organizational culture of highly innovative organizations.

Current and Future Trends for Key U.S. Commercial Industries

Environment, Energy, and Agriculture

As its economy has grown, China's environment has been severely degraded, with the demands for energy, land, and materials outstripping available resources. The country recently declared a "war on pollution" to clean the country's choked skies and waterways.[6] Soil pollution has reduced agricultural output, degrading more than 40% of China's arable land and making China more and more heavily reliant on imported food.[7] Securing adequate natural resources, reversing or stemming environmental damage, and enhancing food security are now national priorities.

Consequently, we expect this reality to increasingly drive Chinese APT groups' attempts to pilfer U.S. technology and expertise. Some examples of the APT trends we have observed include the following:

- Environmental damage has dramatically reduced agricultural output in China, transforming food security into a key concern for leadership. It may also be driving cyber espionage activity. Last summer, FireEye saw one Chinese APT group target four different companies involved in farming, agricultural chemical manufacturing, and agricultural equipment manufacturing.

- Reliance on coal for electricity generation is the main culprit of China's poor air quality, resulting in plans to construct 13 new nuclear power plant reactors by 2018.[8] In 2012, shortly after the Chinese government released its nuclear energy safety strategy, FireEye observed one of the most sophisticated Chinese threat groups we track conduct an espionage campaign targeting companies in niche parts of the nuclear industry.

- Breakthrough renewable technologies are all but guaranteed to top Beijing's list of technology acquisition priorities. We expect that companies with experience in solar panel and wind power turbine technology (in which Chinese companies already used pilfered technology to undercut foreign competitors)[9] will occur with electric vehicles, emission reduction technologies, battery development, and other energy-saving products. In 2014 FireEye observed a China-based group steal data from a company involved in some of these niche renewable energy technologies.

Future-Oriented Technologies, Surveillance, and Big Data

Manufacturing still remains one of China's key economic drivers, and the Chinese leadership clearly recognizes the potential of next-generation technologies. Our analysts have observed approximately 20 different Chinese APT groups target companies involved in next-generation IT

and high-end equipment manufacturing. One instance included the targeting of an electronics organization specializing in law enforcement-related surveillance technologies that probably support the government's push to ensure domestic security and otherwise monitor the populace.

China has set the goal of leading the world in the "Internet of Things," earmarking $800 million for investment by 2015.[10] [11] Chinese companies are also making rapid strides in artificial intelligence.[12] Looking forward, we expect to see further attempted data theft of R&D related to the Internet of Things, artificial intelligence and robotics, big data, and 3D printing.

Healthcare and Pharmaceuticals

Facing critical challenges in the public health and pharmaceutical sectors, the Chinese leadership seems again to have turned to cyber espionage. We believe this activity is ultimately geared towards advancing domestic champions, and possibly to prepare firms for foreign ventures and partnerships. China seeks to implement universal healthcare by 2020, and there are definite concerns over rapidly rising healthcare costs.[13] Spending on pharmaceuticals in China is expected to exceed $107 billion in 2015, and China will be the world's second-largest drug market by 2020.[14] A series of demographic shifts leading to an aging population with growing obesity, cancer, and hypertension rates only adds urgency to the healthcare problem.[15] [16] [17]

FireEye has observed more than eight Chinese APT groups pursue victims in the pharmaceutical and healthcare industries, successfully targeting business and strategic plans and goals, as well as information from human resources and legal departments. We have seen some APT groups pursue specific, cutting-edge research and intellectual property related to certain critical health challenges. For instance, one APT group has extensively tried to target oncology-focused biotechnology.

Targeting Personal Data

Intellectual property and business information is not the only type of data in which targeted threat groups have shown an interest, although it is by far the most frequently stolen. It appears that advanced cyber threats, some of which may be based in China, have stolen significant amounts of personal data from several different organizations in the past year.

The motivations for stealing this type of information are not yet entirely clear. It is possible that this interest in personally identifiable information and related data is ultimately for monetary gain and criminal purposes, as we know that some threat actors operate as contractors. In fact, we classify at least 3 of the groups we track as operating on a contract-for-hire basis.

Another working hypothesis is that the stolen information could be used for broader espionage purposes, such as to better facilitate follow-on activity by identifying specific individuals, or to make more effective social engineering campaigns.

It is still too early to make a determination, but these developments certainly underscore that the threat landscape is constantly evolving.

Conclusion

China-based cyber espionage actors will likely continue to target U.S. industries in the growth

areas that we have described above. Since it is extremely difficult for even security conscious companies to withstand a targeted attack from a nation state, we recommend that companies prepare to respond rapidly to a breach in order to minimize the impact or adverse consequences.

In January 2015, we released an annual threat report that presents insights, statistics, and analysis drawn from the combined experience of our Incident Responders. This year's report portrays a threat landscape that is more complex than ever, with security teams finding it increasingly difficult to prevent, detect, analyze, and respond to advanced attacks. Some highlights from this report include the following:

- On a positive note, the time it takes organizations to discover compromises continues to drop. The median number of days attackers were present on a victim's network before being discovered dropped to 205 days in 2014 from 229 in 2013 and 243 in 2012; however, this is still too long and some breaches can go undetected for years. In an extreme case, we identified one organization that had been breached for over eight years without knowing.

- However, it is becoming more and more difficult for organizations to detect breaches on their own. In 2014, only 31 percent of organizations discovered via their own resources that they were breached – down from 33 percent in 2013 and 37 percent in 2012.

- Attackers have also improved their counter-forensics, and as a result, they are more capable of concealing their activities by leaving less evidence behind, posing a challenge for both detection and incident response.

These trends are likely to continue for the foreseeable future, particularly in light of the rapid adoption of mobile and cloud computing technologies, which provide advanced cyber threats with additional attack vectors.

---

[1] Department of Justice; Office of Public Affairs. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." May 19, 2014. <http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>

[2] "State Council 12th Five Year Plan (FYP) on Development of Strategic Emerging Industries." July 2012. <http://www.gov.cn/zwgk/2012-07/20/content_2187770.htm>

[3] "Xi Says China Must Adapt to 'New Normal' of Slower Growth." *Bloomberg*. May 11, 2014. <http://www.bloomberg.com/news/articles/2014-05-11/xi-says-china-must-adapt-to-new-normal-of-slower-growth>

[4] Sharma, Yojana. "What do you do with millions of extra graduates?" *BBC*. July 1, 2014. <http://www.bbc.com/news/business-28062071>

[5] Riley, Michael A. "Chinese Hackers Force Penn State to Unplug Engineering Computers." *Bloomberg*. May 15, 2015. <http://www.bloomberg.com/news/articles/2015-05-15/china-hackers-force-penn-state-to-unplug-engineering-computers>

[6] "China to 'declare war' on pollution, premier says." *Reuters*. March 4, 2014. <http://www.reuters.com/article/2014/03/05/us-china-parliament-pollution-idUSBREA2405W20140305>

[7] Patton, Dominique. "More than 40 percent of China's arable land degraded: Xinhua." *Reuters*. November 4, 2014.

<http://www.reuters.com/article/2014/11/04/us-china-soil-idUSKBN0IO0Y720141104>
[8] Graham-Harrison, Emma. “China warned over 'insane' plans for new nuclear power plants.” *The Guardian*. May 25, 2015. <http://www.theguardian.com/world/2015/may/25/china-nuclear-power-plants-expansion-he-zuoxiu>
[9] Cardwell, Diane. “Solar Company Seeks Stiff U.S. Tariffs to Deter Chinese Spying.” *New York Times*. September 2, 2014. <http://www.nytimes.com/2014/09/02/business/trade-duties-urged-as-new-deterrent-against-cybertheft.html>
[10] Voigt, Kevin. “China looks to lead the Internet of Things.” *CNN*. December 3, 2012. <http://www.cnn.com/2012/11/28/business/china-internet-of-things/>
[11] Ibid.
[12] Zhang Rui. “Baidu CEO proposes national AI project.” March 12, 2015. <http://www.china.org.cn/china/NPC_CPPCC_2015/2015-03/12/content_35030729.htm>
[13] Franck Le Deu, Rajesh Parekh, Fangning Zhang, and Gaobo Zhou. “Health care in China: Entering ‘uncharted waters.’” McKinsey. November 2012. <http://www.mckinsey.com/insights/health_systems_and_services/health_care_in_china_entering_uncharted_wate>
[14] Wang, Shirley S. “A New Cancer Drug, Made in China.” *Wall Street Journal*. April 2, 2015. <http://www.wsj.com/articles/a-new-cancer-drug-made-in-china-1428004715>
[15] “ Ageing China: Changes and challenges.” *BBC*. September 20, 2012. <http://www.bbc.com/news/world-asia-19630110>
[16] Pang Li. “Obesity is a growing concern in China.”. <http://www.china.org.cn/china/2012-09/14/content_26521029.htm>
[17] French, Paul, “Fat China: how are policymakers tackling obesity.” *The Guardian*. February 12, 2015. <http://www.theguardian.com/global-development-professionals-network/2015/feb/12/chinas-body-mass-time-bomb-policymakers-tackling-rising-obesity>