CHINA'S ESPIONAGE DYNASTY

ECONOMIC DEATH BY A THOUSAND CUTS

AUTHORS:

JAMES SCOTT (ICIT SENIOR FELLOW – INSTITUTE FOR CRITICAL INFRASTRUCTURE TECHNOLOGY)

DREW SPANIEL (RESEARCHER AT THE INSTITUTE FOR CRITICAL INFRASTRUCTURE TECHNOLOGY)

ICIT Institute for Critical Infrastructure Technology

ICIT Briefing: **China's Espionage Dynasty**

July 28, 2016
Washington D.C.

Join ICIT experts as we discuss the findings of this publication and identify solutions to protect our critical infrastructures and our way of life.

http://icitech.org/event/chinese-advanced-persistent-threat-groups/

Authors:

- James Scott, Sr. Fellow, ICIT
- Drew Spaniel, Researcher, ICIT

Expert research contributed by the following ICIT Fellows:

- Ryan Brichant, ICIT Fellow & CTO, Critical Infrastructure, FireEye
- John Sabin, ICIT Fellow & Director, Network Security and Architecture, GRA Quantum

ICIT | Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Contents

Introduction

The criminal culture of theft that has been injected into virtually every line of China's 13th Five-Year Plan is unprecedented. From state sponsored smash and grab hacking and techno-pilfering, to corporate espionage and targeted theft of IP, the threat is real, the economic implications are devastating and Western Nations are the primary target of China's desperate effort to steal in order to globally compete. Never before in recorded history has IP transfer occurred at such a rapid velocity.

The all-encompassing, multifaceted onslaught of cyber-physical Chinese espionage targets industry genres from satcom to defense and from academic research to regional factories manufacturing proprietary blends of industrial materials. China seeks to not only steal but to economically interrupt and cripple. Economic warfare is just as much a part of the strategy as catching up to Western innovation and becoming less dependent on foreign technology. Chinese student and scholar associations, trade organizations, legions of strategically placed insider threats and yes, even criminal organizations such as the Triad, all play their key role in the purloining of intellectual property in contribution to the Chinese agenda. This report covers the primary structure of Chinese espionage initiatives.

China's Thirteenth Five-Year Plan

China's Thirteenth Five-Year Plan (2016-2020) focuses on cutting edge technology and socio-economic reform. The plan calls for innovative technology to improve national infrastructure and more environmentally friendly technology to alleviate China's ecological footprint. By 2025, China wants to improve its national technological core, reduce the global perception that its products are of inferior quality (likely by improving their quality by modernizing the underlying manufacturing infrastructure), and diversify its domestic industrial markets. While China will develop some of the technology necessary to aspire towards these goals as the result of the intellectual endeavors of its people, the majority will likely be obtained as stolen intellectual property from the United States and other nations. As ICIT Fellow John Sabin (GRA Quantum) observed "When you understand China's desire to be a global leader across markets, you can rationalize their preference to simply steal intellectual property. Say, for example, they want to become the world leader in pharmaceuticals. Instead of investing billions of dollars supporting science education and the development of a robust and innovative biomedical industry, China can simply leverage what it already has a competitive advantage in – hacking – and steal an American company's drug formula in a fraction of the time." The remainder of the plan focuses on balancing welfare gaps and bridging socio-economic differences. Since it is unlikely that the Chinese Communist Party (CCP) will reform its structure to support a more inclusive approach to governance, attempts at improving the standard of living of the Chinese people will likely be gleaned from organizational, structural, and operational models created from dossiers and data exfiltrated from systems belonging to Western organizations. In short, like its predecessors, a majority of China's Thirteenth Plan depends on sustained espionage against countries like the United States, Canada, and Australia.

Economic Impact of Intellectual Property Theft

The United States is built upon an intangible economy. Gone are the days when American currency was backed by gold or silver; now, it is backed by ideas. The entire United States economy relies on some form of intellectual property because every industry either produces or uses it. In their March 2012 *Intellectual Property and the U.S. Economy: Industries in Focus* report, the Economics and Statistics Administration of the U.S. Patent and Trademark Office identified 75 out of 313 industries as IP -intensive. These accounted for 27.1 million jobs, or 18.8% of all employment in 2010. 12.9 million more supply chain jobs were indirectly supported by intellectual property. IP-intensive industries accounted for $5.06 trillion in value added or roughly 34.8 % of the U.S. GDP in 2010. Some researchers estimate that as much as an immediate $300-500 billion and 1.2 million jobs are lost every year due to the theft of intellectual property. These costs may be much greater in consideration of the losses over the potential lifetime of the property.

In September 2015, President Obama and President Xi Jinping revealed in a joint media conference that the United States and China had reached a deal that neither government would conduct cyberattacks to steal intellectual property for economic gain from the other. The agreement recognized that neither Obama nor Xi could guarantee the actions of all their citizens. Many security researchers and legislators doubted that the agreement would alter the behavior of China in cyberspace. In late June 2016, FireEye's Ryan Brichant commented, "Since mid-2014, we have seen a notable decline in China-based groups' overall intrusion activity against entities in the U.S. and 25 other countries. We suspect that this shift in operations reflects the influence of ongoing military reforms, widespread exposure of Chinese cyber operations and actions taken by the U.S. Government. In 2013, FireEye observed 70 active network compromises by China-based groups each month. In 2015, we observed less than 10 active network compromises. In 2014, the U.S. Government began to take unprecedented measures in response to claims of Beijing's cyber-enabled economic espionage. Although many in the U.S. initially doubted that these actions would have any effect, they may have prompted Beijing to reconsider the execution of its network operations. We have not seen evidence of a coordinated shift in the behavior of recently active China-based groups; tactical changes appear to be specific to each group's mission and resources, and in response to public exposure of its cyber operations." While it is possible that China has reduced its targeted attacks against American organizations, it seems more likely that it restructured its cyber operations to assert greater control over its operatives.

Prior to the agreement, the Chinese cyber army operated on several tiers. The first tier consists of the members of the Third Department, state-sponsored APT groups, and other cyber professionals, hired by the military to conduct offensive and defensive cyber operations. The second tier consists of specialists in civilian organizations, such as the Ministry of State Security or Ministry of Public Security, who are authorized by the military to conduct cyber operations. The third tier consists of external groups that can be hired or mobilized to conduct cyber operations. This would include cyber criminals, mercenary groups, and script kiddies who occasionally work with the higher tiers. Finally, beneath all the tiers are an estimated 500,000 paid propaganda proponents and other internet users who promote the Chinese Communist Party and its leaders, while criticizing its enemies online. The People's Liberation Army (PLA) does not fully cover the operating expenses and modernization funds of the departments. Prior to the agreement, the departments supplemented budgets with other activities, such as conducting cyberattacks. When Xi Jinping announced at the beginning of September 2015, that he was cutting 300,000 troops, his intent was multi-purposed. On one hand, he may have planned to purge the military of less loyal members and on the other hand, he focused the departments and ordered them to cease extra ventures, such as sloppy cyberattacks, that could result in economic sanctions against China. This also could have resulted in less work for the lower tiers as Chinese state cyberattacks would be more professional, more difficult to detect, and more focused on high priority targets. It is possible that the financially motivated attacks were simply redirected. Kaspersky Lab alleges that in response to the agreement, Chinese APT attacks against Russian targets increased 300 percent between December 2015 and February 2016. In further support of the possibility that the agreement either spurred fiscal operations out of the government or incited outsourcing, evidence suggests that the early 2016 increase in ransomware attacks may have been conducted by Chinese operatives. Four separate security firms concluded that tools and tactics previously associated with Chinese government-supported cyber-intrusions were used in some attacks.

It is important to recognize that the September agreement only pertains to attacks conducted for economic gain. Neither nation is barred from launching cyberattacks intended to steal intellectual property or data for any other purpose, such as the development of infrastructure, military, or technology capabilities. Traditional espionage attacks against government organizations, such as OPM, Anthem, or federal databases, are not addressed by the agreement. Even if the agreement did holistically address cyberattacks, it would be difficult to prevent the first tier from outsourcing attacks to the lower tiers.

The Structure of Chinese Espionage

The Central Committee of the Chinese Communist Party (CCP) is the political body consisting of the most powerful members of the Communist Party of China. The Committee is the highest authority when the National Congress is not in session. The Central Committee is comprised of 205 full members and 171 alternate members. The Central Committee conducts intelligence operations through a covert and an overt spy structure.

Covert Spy Structure

The CCP controls the People's Liberation Army through a Central Military Commission (CMC). The Commission is the parallel national defense agency of the Communist Party of China and the People's Republic of China. The CMC is an 11-man commission and its chairman is the commander-in-chief of the armed forces, Xi Jinping at the time of this writing. The CMC sets military policies and issues directives relating to the PLA.

Joint Staff Department

The People's Liberation Army (PLA) Joint Staff Department (JSD) replaced the General Staff Department on January 11, 2016 as part of Xi Jinping's military reforms. It manages the majority of military and covert operations. The JSD, as a division of the PLA, is dedicated to warfare. The duties of the PLA JSD include PLA Operations Command, Recruitment, Mobilization, Formation, Training, and Administration. The JSD contains three departments, which cooperate to conduct intelligence operations. The fact that human intelligence, signal intelligence, and electronic intelligence are all housed under the same, military department demonstrates that the Chinese view the modern threat landscape as a cyber-physical battlefield.

Second Department

The Second Department handles conventional human intelligence (HUMINT), such as high-level spies and intelligence assets. A common misconception is that agents of Chinese government are "sloppy"; however, agents of the second department who serve as high-level spies or handlers are rarely caught. Rather, low-level assets, often belonging to the overt structure are more often detected by foreign intelligence agencies. It is believed that the Second Department consists of 30,000- 50,000 human spies who are operating as insider threats within various foreign organizations.

Under the current Five Year Plan, much of the Second Department's efforts are focused on the aggregation of intellectual property and intelligence. In some cases, agents of the second department operate in concert with hackers and APT groups in the Third Department, by acting as insider threats or otherwise facilitating the compromise of target systems.

Third Department

The Third Department is responsible for signals intelligence (SIGNIT). The Third Department is the largest intelligence agency in the Chinese government, consisting of an estimated 250,000- 300,000 linguists, technical staff, and cyber soldiers. There are at least four known Research Institutes (56, 57, 58, and 61) under the Third Department. Within the 61 Research Institute are approximately 20 bureaus that launch cyberattacks. The Third Department intercepts phone calls, launches cyberattacks, and monitors communications. Much of its efforts involve hacking devices and exfiltrating targeted data. The Third Department may launch obvious cyberattacks, such as DDoS or ransomware attacks, against target systems to mask the activity of Second Department operatives.

Fourth Department

The Fourth Department conducts electronic intelligence (ELINT) operations and is focused on intercepting satellite and radar data. Fourth Department operations might involve altering, jamming, or spoofing signals. It is believed that the Fourth Department researches direct methods of disabling enemy communication networks.

State-Sponsored APTs

Chinese state sponsored advanced persistent threats can be identified based on their choice of targets, their proclivity for cyberespionage, and the language settings on the keyboards used to develop the malware, and their connections to other campaigns. Some groups, such as APT 1 (Unit 61398), APT 2 (Unit 61486) and APT 30 (Unit 78020) can be linked to specific units within the Third Department. Other APTs remain less defined. Below are some brief profiles of Chinese APTs. Despite the catalog below and those included in ICIT's *Know Your Enemies* reports, even more Chinese state-sponsored APTs remain undiscovered at the time of this writing.

PLA Unit 61398/ APT 1/ Comment Panda/ Comment Crew/ TG-8223

In 2013, Mandiant published their 60-page report, *APT 1: Exposing One of China's Cyber Espionage Units*, detailing the activities and location of a Chinese state-sponsored advanced persistent threat and associated organizations that were conducting cyberattacks against American organizations and government agencies from a 12-story building on the outskirts of Shanghai. APT 1, or Unit 61398, is the Second Operational Bureau of the Third Department of the People's Liberation Army (PLA) General Staff Department (GSD). It operates from four large networks in Shanghai, two of which serve the Pudong district of Shanghai. Additionally, the Chinese government provides a direct fiber optic connection to the facility in the name of national defense. On May 19, 2014 a Federal grand jury indicted five officers of Unit 61398 (Huang Zhenyu, Wen Xinyu, Sun Kailiang, Gu Chunhui, and Wang Dong) on charges of compromising American systems and stealing intellectual property. Federal prosecutors listed some suspected targets as Alcoa Inc., Allegheny Technologies Inc., United States Steel Corp, the Toshiba Corp unit of Westinghouse Electric Co, the U.S. subsidiaries of SolarWorld AG, and a steel workers' union. The indictment alleges that Chinese state-owned companies hired Unit 61398 to provide information technology services, including assembling a database of corporate intelligence, concerning the targets. The use of a military signal intelligence division to aid state owned businesses demonstrates a clear difference between strategic cyber operations in the United States versus China. The United States relies on its cyber operations for defense and some military intelligence; meanwhile, China utilizes its cyber capabilities for business, socio-economic, and military purposes.

Unit 61398 targets sectors that are of interest to China's current Five Year Plan. Primary targets include intellectual property, trade secrets, financial data, organizational data or systems in the Information Technology, Aerospace, Defense, Energy, Manufacturing, Public Administration, or other governmental or technical sectors. It is large enough and well-resourced enough that it can simultaneously compromise dozens of organizations. Attacks from the group may date back as early as 2002. At the very least, the group has attacked over a thousand corporations and government entities across the globe since 2006. At least several hundred of those attacks have resulted in severe breaches. The majority of the targets have been American; however, Dell Secure Works and other firms allege that the group has also targeted systems belonging to the United Nations, Canada, South Korea, Taiwan, and Vietnam.

APT 1 received some of its names, such as Comment Crew, Comment Panda, and similar titles, due to its tendency to infiltrate organizations by compromising the "comment" features of legitimate web applications in order to laterally navigate to internal applications or systems. More recent attacks have used personalized spear phishing emails that contain a malicious file or link. Attachments are usually ZIP files.

Once the victim system is compromised, the attacker establishes a persistent presence by installing a backdoor from the dropper delivered from the email. The backdoor bypasses internal security by contacting C2 infrastructure from inside the network. The actor typically relies upon WEBC2 or BISCUIT backdoors. WEBC2 is a minimally featured beachhead backdoor that can only communicate with a C2C server through comments. BISCUIT backdoors are used if more functionality is needed. BISCUIT uses the HTTP protocol for communication and it features modules to capture screenshots, log keystrokes, record system information, modify processes, modify the registry, execute code, log off or shut down the session, and other features. Unit 61398 remains persistent on the compromised system for months or years. During this time, the group gathers login credentials from publicly available tools built into the initial malware and escalates account privileges, conducts network reconnaissance and laterally explores the network to infect new systems. Unit 61398 compresses stolen data into multiple files with a RAR archiving utility and exfiltrates the data through their backdoor or through File Transfer Protocol (FTP).

PLA Unit 61486/ APT2/ Putter Panda/ TG-6952

The advanced persistent threat known as Putter Panda, or PLA Military Unit Cover Designator (MUCD) 61486, is internally known as the People's Liberation Army's (PLA) Third Joint Staff Department (JSD) Twelfth Bureau. The group has been active since at least 2007 and it is based out of the Zhabai district of Shanghai. Unit 61486 shares some infrastructure with Unit 61398. Analysts of Project 2049 Institute allege that Unit 61486 supports China's space surveillance network and maintains close ties with the state-sponsored Beijing Remote Sensing Research Institute, whose mission is to explore "leading technologies in earth observation and the mechanisms for acquiring and distributing remote sensing information." The cyber targets of Unit 61486 tend to be affiliated with satellite, aerospace, or defense technologies.

Much like Unit 61398, Putter Panda targets intellectual property, trade secrets, and other data related to government entities, the Aerospace sector, the Defense sector, the Communication sector, the Technologies sector, and research facilities. According to CrowdStrike, the United States Defense industry, communication industries, and European satellite and aerospace industries are particularly targeted.

Like most APTs, Putter Panda relies on spear phishing emails containing malicious PDFs and Microsoft Word Documents to infect target systems. Its exploit kit includes two droppers, two RATs, and two tools. One dropper delivers a payload, such as the 4H RAT, to the victim system and installs it. The other dropper exclusively delivers the PNGDOWNER tool. Putter Panda uses the 4H RAT and the 3PARA RAT. The 4H RAT can initiate a remote shell, enumerate running processes, terminate processes, list files and directories, modify timestamps, upload files, download files, and delete files. The RAT communicates over HTTP and the communication is obfuscated by an operation, 1-byte XOR with the key 0xBE. The 3PARA RAT is a second stage, failsafe tool that allows the attacker to regain control of the system if their initial access vector is removed. The 3PARA RAT creates a file map at startup to verify that there is not another instance of the RAT running. The RAT is capable of remaining dormant for prearranged or commanded periods of time. The RAT only has limited commands, which include retrieving file or disk metadata, changing the working directory of the current C2 session, executing a command, and listing the current working directory. The first tool, PNGDOWNER is a simple download and execute tool. The second tool, HTTPCLIENT is a backup tool. The 3PARA RAT communicates over HTTP and authenticates with a 256-byte hash and a hard-coded string.

Deep Panda/ APT 19/ Shell Crew/ Black Vine/ Kung Fu Kitten

According to Symantec, Crowd Strike, and other security firms Deep Panda is a Chinese state-sponsored threat actor that began attacking the Healthcare, Aerospace, and Energy sectors around 2012.

Deep Panda attacks tend to have massive impacts and they accrue proportional media attention. In order to conduct multiple sizable campaigns against United States Federal government agencies and major western health care providers for extended time periods, Deep Panda must have considerable resources at their disposal. In illustration, it is possible that Deep Panda was concurrently engaged in cyber-attacks against the United States Office of Personnel Management, the Anthem healthcare network, United Airlines, and other entities. A vast majority, ~80%, of Deep Panda targets are American.

Prior to 2012, there are indications that China did not target PII; however, Deep Panda and affiliated groups, such as Axiom, now regularly exfiltrate PII and healthcare data. The information is rarely, if ever, exploited for financial gain. Instead, the shift in targeted information could indicate the likelihood that the information is valuable for the creation of dossiers, monitoring systems, or to leverage against individuals who concern the Chinese government.

In the United States Healthcare sector, Deep Panda has attacked VAE, Anthem, Empire Blue Cross Blue Shield, and Carefirst. In the recent 2014-2015 Anthem breach, the group exfiltrated ~80 million patient records. Information exfiltrated from Anthem includes social security numbers and other personal identifiable information or personal health information. It is believed that the Axiom group also attacked Anthem at the same time as Deep Panda, but with a different malware and along different vectors. The attack appears to be affiliated. Further, enough similarities exist between the meticulous planning and malware employed by the two groups that many security firms hypothesize that they are both part of the same group. There is a strong possibility that the groups are parts of a coordinated effort under the Chinese government.

Deep Panda is believed to be responsible for the two 2015 OPM breaches. Further, Deep Panda breached United Airlines in 2015 and stole departure and destination records. The health, OPM, and travel records stolen by Deep Panda can be aggregated to catastrophically impact the United States government over time. The adversary or their parent nation-state, can use the stolen information to build a database of US employees for espionage purposes. The information can also be used to identify United States agents in the country or to identify Chinese assets who assist United States intelligence efforts. Moreover, the information obtained in the OPM breach could be combined with the information stolen in Deep Panda's healthcare breaches or with information publically released in incidents, such as the Ashley Madison breach, to manipulate or leverage pressure against specific United States citizens to serve the Chinese agenda.

PLA Unit 78020/ APT 30/ Naikon

The Naikon group is allegedly a state sponsored hacking unit of the PLA, that has been charged since 2010 with collecting intelligence from political and military targets to advance China's interest in the South China Sea. The threat actor is known for spear-phishing campaigns against civilian, military, and government organizations in the Philippines, Malaysia, Cambodia, Indonesia, Vietnam, Myanmar, Singapore, Nepal, Thailand, and Laos. Many of these countries have strong ties to the ASEAN Union or the United States. China desires control of the South China Sea because it relies heavily on shipping routes through the region. The Unit 78020 campaign indicates a marriage of cyber intelligence with physical strategic action. The connection of Naikon to the PLA is the result of security researchers identifying one of its members as a military researcher named Ge Xing.

Spear phishing campaigns begin with a lure email relevant to the victim that carries a malicious Microsoft Word document, which, according to Kaspersky Lab, actually contains "a CVE-2012-0158 exploit, an executable with a double extension, or an executable with an RTLO filename". The vulnerability is a buffer overflow in the ActiveX controls of the MSCOMCTL.OCX Windows library. The exploit is used to install a RAT which in turn plants a backdoor on the system.

One of Naikon's most prolific spear phishing campaigns was the March 2014 attacks against organizations from countries affected by the MH370 tragedy. Upon opening/ execution, the malicious payload, an 8kb encrypted file and configuration data, was injected into the browser memory where it decrypted the ports and paths to the C2C server, a user agent string, filenames and paths to relevant components, and hash sums of the user API functions. The malicious code downloaded the main malware from the C2C server over an SSL connection and then it loaded it independently of the operating system functions without saving it to the hard drive by assuming control of the XS02 function and then handling the installation in memory.

The main component of the Naikon platform is a remote administration component. According to Trend Micro, the RARSTONE backdoor (BKDR_RARSTONE.A) can obfuscate itself by "decrypting and loading a backdoor 'executable file' directly into memory without the need to drop the actual 'executable file.'" The backdoor installs like a Plug X backdoor, injecting code into hidden instances of internet explorer. The module establishes a connection to the C2C server to receive and execute any of an estimated 48 commands from the adversary on the host. These commands include profiling the system, uploading and downloading data, executing arbitrary code, installing other modules, or executing commands via the command line. The backdoor routine also has the ability to get installer properties from Uninstall Registry key entries, which allow it to silently uninstall applications that interfere with the malware. The espionage malware collects email messages, monitors victims keystrokes and screens in real time, and monitors network traffic.

Axiom/ Winnti Group

The Axiom group is a Chinese, state-sponsored, threat actor that has targeted information systems that store information relevant to China's Thirteenth Five Year Plan since 2009. Until 2013, the APT primarily targeted intellectual property such as source code and internal systems design belonging to gaming companies, as well as the digital certificates used by those companies. Targeting gaming companies, especially in the massive multiplayer role-playing game (MMORPG) space, enables the threat actors to target millions of users worldwide. Additionally, the theft of authentic digital certificates enables the threat actor to sign and distribute malicious code as if it were legitimate. Afterward, it began to attack the pharmaceutical sector and now, Axiom targets law enforcement, governmental records and communication agencies, environmental policy agencies, personnel management divisions, space and aerospace exploration and research entities, and government auditing and internal affairs divisions. In the science and technology sectors, Axiom targets networks belonging to electronics and integrated circuitry manufacturers, networking equipment manufacturers, internet based service companies, software vendors, cloud computing companies, energy firms, meteorological service companies, telecommunications firms, and pharmaceutical companies. Additionally, Axiom has targeted journalism and media outlets, Human Rights NGOs, international law firms, international consulting and analysis firms, and high-ranking United States academic institutions. Most of the target's organizations have been located in the United States, South Korea, Taiwan, Japan, and the European Union, with a majority of the breaches along the Eastern seaboard of the United States and Western Europe.

Axiom campaigns share infrastructure, malware, or attack techniques with Operation Aurora (2009), the Elderwood Project (2009-2014), the VOHO campaign (2012), the Shell_Crew attacks on ColdFusion servers (2013), Operation Ephemeral Hydra (2013), Operation Snowman (2014), and 2014 attacks on American Middle Eastern Policy think tanks. Axiom could be connected to some of these other groups; however, it is more likely that Axiom advantageously adopts zero-day exploits or malware that are effective in other campaigns.

Axiom is likely Chinese state sponsored, but there is no indication whether it is operated by a military unit or by mercenary attackers. Axiom is more sophisticated in its operations than the aforementioned Third Department groups. It utilizes different resources, and it may have a different mission than Third Department groups. Novetta hypothesizes that based on Axiom's domestic monitoring trends it might be charged with domestic operations and targeting Chinese dissidents in other countries. Universities and research institutions in Hong Kong and mainland China have been targeted with Hikit malware for persistent operations. This could indicate state-sponsored concern over liberal academics and students.

Axiom targeting coincides with interests reflected in China's Five-Year Plans, which push for advanced technology and advanced R&D efforts. As China shifts away from foreign technology, more organizations may be targeted by Axiom. The actor may target semiconductor and networking technology firms with offices in China because China wants to reduce its dependency on foreign technology. Western and Asian organizations may be targeted in intelligence and counterintelligence operations. Axiom targets NGOs concerned with international politics, environmental policy, pro-democracy movements, or human rights movements. In some instances, Axiom will target a satellite office and move laterally through the compromised network to the main office. Novetta theorizes that Axiom targets NGOs as a means of the Chinese ruling party keeping track of watchdog organizations and other groups who may publish claims that challenge the authority or "soft power" of the party. Targeting NGOs may also enable the party to suppress dissidents or intimidate whistleblowers.

Novetta believes that Axiom has a six stage victim lifecycle that uses a different team for each stage of the attack. This indicates large scale organization and coordination. Initially, the target is identified and the actor conducts reconnaissance. Then the system is compromised, confirmed to be a valuable target, and surveyed. The actor laterally moves through the network and creates additional footholds. Compromised C2 infrastructure is connected to the victim network. Finally, valuable data is identified and exfiltrated.

Axiom initially compromises systems through web based attacks, targeted attacks against public facing infrastructure, zero-day exploits, watering hole attacks, and phishing emails. Once a system is compromised, Axiom spends a few days determining whether it is valuable. If it is determined to contain useful information, then the group installs persistent malware platforms. Otherwise, the group tries to move laterally through the network to locate more valuable systems. Axiom has proven capable of compromising large pools of machines and sifting through them in hours or days to find the valuable ones. This indicates dedicated resources, possibly a dedicated targeting team and a deterministic set of criteria.

After the initial compromise, Axiom begins reconnaissance to identify where they are in the target network and to identify any changes that have been made to the network. Axiom then escalates privileges using previously compromised administrative accounts, local exploits, or remote exploits as demonstrated in ZoxRPC malware. Then, over the course of minutes or months, they try to dump the latest user credentials and exfiltrate the data. Once inside the network, Axiom can also exploit Remote Desktop Protocol or exploit vulnerabilities in the custom tools designed by the organization itself. This allows Axiom to obfuscate its presence from antivirus or IDS systems.

As the campaign continues, Axiom may install additional families of malware as a mechanism of remaining in the system even if one malware is discovered by the target. Compromised systems have featured up to four layers of malware ranging from extremely common (Poison Ivy, Gh0st, ZXshell) to focused tools used by threat groups (Derusbi, Fexel) to custom Axiom malware (ZoxPNG/ZoxRPC, Hikit). Axiom routes its activity through compromised proxy infrastructure in the United States, South Korea, Taiwan, Hong Kong, and Japan to try to disguise its traffic as legitimate to casual observation.

Novetta observes that the Hikit malware is unique to Axiom and is only used on high value targets at the height of the victim's operational lifecycle. Of the 43,000 compromised systems discovered in Operation SMN, only 180 systems were infected with the Hikit malware. Hikit is a late stage persistence and data exfiltration tool that is capable of uploading and downloading files, generating a remote shell, tunneling into the network, and connecting to other infected machines to generate a secondary network.

Hurricane Panda

The Hurricane Panda group targets internet services, engineering, and aerospace companies in an attempt to steal confidential data and intellectual property.

Hurricane Panda leverages zero-day vulnerabilities, a DNS resolution exploitation technique, and a unique toolkit to access victim networks. The group also leverages SQL injection vulnerabilities, at least three privilege escalation exploits and a remote code execution exploit. Once inside a network, it moves laterally onto a desired system and establishes an RDP session. On some victim systems, the attacker installed the remote access trojan (RAT) kit or the Chopper webshell, which provides the functionality of a RAT on webservers. The RATs employed by Hurricane Panda have been exclusively tied to other Chinese threat actors. Notably, the Sakula malware is closely connected to the Deep Panda group, the Gh0st RAT has been tied to both Axiom and Hidden Lynx, the PlugX malware is connected to the PlugX group, and the Hikit malware is used by Axiom. Additionally, indicators of compromise linked to Aurora have been found on some networks infected by Hurricane Panda, suggesting some level of connections between the groups.

Hurricane Panda extensively used the PlugX tool against the California based Hurricane Electric's free DNS service to resolve their traffic to popular domains. This led incident responders to see the traffic as originating from sites like Pintrest, Github, Adobe, and other legitimate sites. After the threat actor established a persistent presence on a victim host, they steal legitimate credentials using tools like Windows Credential Viewer, Windows Credential Editor, or Mimikatz. Afterward, the adversary reduces their footprint by using the credentials to directly connect to the network and masquerade as VPN users instead of relying on the RAT. If credentials cannot be obtained, then the group establishes an RDP connection using a reverse RDP tunneling capability. Hurricane Panda follows the same exfiltration methodology as most Chinese actors. Targeted files are compressed and password protected using RAR. Then the files are moved to a convenient staging location on the network. Finally, the files are exfiltrated via FTP.

Gothic Panda/ APT 3/ UPS/ Pirpi/ Clandestine Fox/ TG-0110

In early 2014, Gothic Panda began targeting victims in the financial sector, technology industries, NGO/ International arena, aerospace and defense organizations, telecommunication companies, transportation organizations, and the energy sector.

The threat actor typically relies on spear phishing emails to direct targets to a landing page that leverages a use-after-free vulnerability in Internet Explorer. In addition to targeted campaigns, the adversary sent out phishing emails to specialized mailing lists. Topics were related to high-performance computing, weather metadata software, and pre-medical programs at universities. Victims were then infected with the Pirpi malware. The adversary has also recently used zero-day Adobe flash exploits that it obtained in the 2015 Hacking Team breach. The Pirpi backdoor, which features strong detection evasion techniques, is similar to the Dreammon or Dreamclick malware. The two Pirpi variants (one for 2014 and another for 2015) connect to an C2 server and parse returned HTML for commands. The available commands include listing TCP connection status, listing all servers on the domain, gathering network adapter information, downloading files to memory, deleting files, listing directories, uploading files to the C2, executing processes, and other functionalities.

NetTraveler/ Travnet/ Netfile

The NetTraveler APT was discovered in 2013 and is believed to have been active since 2004. The group primarily targets organizations in Mongolia, India, and Russia, though a total of 350-500 infections were detected in 40 countries. Targets are involved in space exploration, Academia, nanotechnology, energy production, nuclear power, lasers, medicine, and communications. Government organizations (19%), private companies (11%), diplomatic organizations and embassies (32%), and military organizations (9%) were also heavily targeted. In recent years, the group has specifically targeted Tibetan and Uyghur activists. The group focuses on cyberespionage and data theft. When Kaspersky Lab investigated the APT, they discovered over 22 gigabytes of stolen data on NetTraveler's C2 servers. The group is believed to consist of around 50 native Chinese members who possess a working knowledge of the English language.

The NetTraveler APT relies on social engineering, watering hole attacks, and zero-day exploits to compromise victim hosts. The infection vectors leveraged Java and Microsoft

Office exploits. After installation, the malware is designed for basic surveillance. It logs keystrokes, cans steal sensitive documents, and it retrieves files system listings.

Mirage/APT 15/ Vixen Panda/ Ke3Chang/ GREF/ Playful Dragon

Since April 2012, the Mirage APT has targeted military and energy organizations in the Philippines, Taiwan, Canada, Brazil, Israel, Egypt, and Nigeria. The most distinct commonality between victims is their involvement in the contest for rights to survey natural gas and oil in the South China Sea. It is believed that the intent of the campaign was to exfiltrate confidential information, steal intellectual property, or to construct a botnet for further infections.

Mirage began attacks with whale-phishing emails, targeting mid-level to senior-level executives with nefarious emails that contain malicious droppers, disguised as PDF attachments, that install the Mirage malware. The dropper executed and copied itself into either C:\ Documents or C:\ Windows directory. The dropper then executed the copy of the malware and terminated the original process. The malware establishes persistence in the event of reboot by creating registry keys and it obfuscates its presence through the creation of one or more files named svchost.exe, ernel32.dll, thumb.db, csrss.exe, Reader_SL.exe, and MSN.exe. The malware profiles the system (MAC address, CPU speed, memory size, system name, and user name) and sends the information back to the command and control infrastructure via an HTTP request over ports 80, 443, and 8080. In some instances, SSL was used for added security. The first variant of Mirage communicated via an HTTP POST request and transferred information that was lightly encrypted by adding each character's ASCII value to its offset from the start of the payload. The second variant of the malware communicated through HTTP GET requests and encrypted data the same way as the former version except that the payload of the initial request is encapsulated in a Base64-encoded string. The Mirage toolkit consisted of a backdoor and a remote access trojan (RAT). At the time of its discovery in 2012, the command and control structure consisted of over 100 domains. By the end of 2012, the Mirage campaign went dormant. However, some of its infrastructure reappeared in the 2015 Hellsing campaign.

Hellsing/ Goblin Panda

The Hellsing group targets government and diplomatic organizations in the APAC region, and nations near the South China Sea. Most targets are from Malaysia, the Philippines, Indonesia, and India. Hellsing was discovered when Kaspersky Lab was investigating the Naikon group and found that Hellsing had responded to a 2014 spear phishing email from Naikon with a custom backdoor. If both Naikon and Hellsing work for the Chinese government, this incident suggests that Hellsing is a mercenary or second tier hacking group; though the same could be said of Naikon. It is not clear whether Naikon intentionally targeted Hellsing or if the incident escalated. Hellsing responded to the spear phishing request for information with a series of questions that pressed upon Naikon's assumed identity (as an employee of the secretariat division of the government of the assumed target nation) and fake credentials. The dialogue and nuance of the exchange indicates that the Hellsing members are more proficient in English than the Naikon group. Finally, Hellsing emailed back a “confidential” locked RAR and the accompanying password. The archive contained two PDFs and a malicious SCR file. The latter file was a backdoor specifically customized to target the Naikon group. Security researchers do not know whether Hellsing infected Naikon.

Hellsing malware samples were primarily compiled in either UTC+6 or UTC+8. Typically, Hellsing infects targets through spear phishing emails containing password protected RAR, ZIP, and 7ZIP archives. Locking the archives bypasses some security features such as Gmail scans. Passwords are included in the emails to the target. Commands to the malware allow the user to upload files, download files, update the malware, and uninstall the malware. After Hellsing establishes a variant of its backdoor, it deploys information-gathering tools. One tool, test.exe, gathers system information and tests available proxies. Another tool, xkat.exe, operates from the Dbgv.sys driver to delete files and kill processes. In addition to operations against victims, the tools may be used to cleanse victim systems of the malware from other APT groups. Each instance of the malware corresponds to a specific C2 server, a version number, and a campaign or victim identifier. Some of the Hellsing infrastructure overlaps with the Mirage APT.

Stone Panda

Crowdstrike identifies Stone Panda as a Chinese APT that has targeted healthcare, aerospace, defense, and government organizations since May 2010. Stone Panda specializes in cyberespionage, network reconnaissance, data exfiltration, and lateral network exploration.

Stone Panda uses spear-phishing to install the PoisonIvy RAT and IEChecker/ EvilGrab tool kit on victim machines. Poison Ivy is a remote administrative tool that is created and controlled by a management kit featuring a graphical user interface. The exploit kit is widely available for purchase or download on the dark net; consequently, its use in high-level campaigns could indicate a lack of technical sophistication of the adversary, who otherwise could have created a custom backdoor utility. Conversely, use of a publically available tool could be an opportunistic or strategic choice as the decision reduces costs to the campaign and complicates profiling attempts due to the ubiquity of the tool. The tool is also used by Axiom and Nightshade Panda.

The PoisonIvy backdoor is copied into the Windows/system32 folder and the filename and installation location are defined by the attacker. Some variants of the malware are capable of copying themselves into an Alternate Data Stream. A registry entry is created to ensure that the malware runs at startup. The malware connects to a server through encrypted and compressed communication and the malware can be configured to inject itself into a browser process before establishing an outgoing connection in order to bypass some firewalls. PoisonIvy gives the attacker complete control over the victim system. The most common operations include: renaming, deleting, uploading, downloading or executing files; viewing or editing registry keys; viewing, suspending, or killing running processes; viewing or terminating network connections; viewing and controlling services; viewing or disabling installed devices; enumerating, deleting, or uninstalling programs. PoisonIvy can steal information by taking screenshots, recording audio or webcam footage, and by capturing saved passwords and hashes. Some variants feature a keylogger and addition functionality provided by third-party plugins.

The EvilGrab exploit kit is spyware that is capable of capturing audio, video, screenshots, and log keystrokes from infected Windows machines. It has three primary components: one .EXE and two .DLL files. The executable acts as the installer. One of the digital libraries is the loader for the other, which is the main backdoor component. Some variants delete the executable after installation. Some variants, such as the IEChecker used by Stone Panda, are capable of stealing credentials stored in Internet Explorer and Outlook. Additionally, some versions are designed to steal information from Tencent QQ, a Chinese instant messaging application or to inject itself into certain security products, such as those distributed by ESET, Kaspersky, and McAfee.

Nightshade Panda

Since February 2008, Nightshade Panda has targeted systems belonging to media corporations, NGOs and international relation organizations, and universities. It shares many similarities to its sister campaign, Stone Panda. Nightshade Panda also specializes in network reconnaissance, lateral network exploration, data exfiltration, and cyberespionage.

Nightshade likely delivers malware through targeted spear-phishing emails. Nightshade Panda relies on the PoisonIvy malware, also used by Stone Panda and Axiom, and on the PlugX malware, used by Naikon. The PlugX malware performs many of the same functions as the PoisonIvy malware, though its more recent development, beginning in 2012 instead of 2008 for the former, may make it preferable for attackers. The malware consists of three components: a legitimate file, a malicious .DLL that is loaded by the legitimate file, and a binary file that contains the malicious code loaded by the .DLL.

PlugX also has features that distinguish it from PoisonIvy. It can also be loaded with several backdoor and other unique modules. XPlugDisk allows the malware to copy, move, rename, execute and delete files. XPlugKeyLogger allows the malware to log keystrokes made on current active windows. XPlugRegedit allows the malware to enumerate, create, delete and modify registry entries and values. XPlugProcess allows the attacker to enumerates processes, collect process information, and terminates processes. XPlugNethood allows the malware to enumerate network resources and set TCP connection states. XPlugService allows the malware to delete, enumerate, modify and start services. XPlugShell allows the malware to perform remote shell on the affected system. The malware also has a debug log file that allows attackers to monitor its performance and troubleshoot issues and errors.

Anchor Panda

Crowdstrike revealed the presence of Anchor Panda at the 2013 RSA conference. Supposedly the APT had launched 124 attacks in the first half of 2013. Most of the attacks were aimed at civilian and military maritime operations in the green/brown water regions in the area of operations of the South Sea Fleet of the PLA Navy. The group also targeted companies in the United States, Germany, Sweden, the UK, Australia, and other nations involved in maritime satellite systems, aerospace industries, and the defense sector. Embassies, diplomatic organizations, foreign intelligence services, and foreign government space programs may also have been targeted. The target of organizations in the South China Sea and in the aerospace sector distinctly align with China's Twelfth Five-Year Plan, which was in place at the time of the attacks. It is believed that the focus of the group is cyberespionage and the theft of confidential data and intellectual property.

Anchor Panda uses the Gh0st exploit kit, which is also employed by Axiom and Hidden Lynx; the PoisonIvy malware, which is used by Axiom, Stone Panda, and Nightshade Panda; the Torn RAT; or a custom backdoor detected by Symantec as the Anchor Panda Backdoor.

Numbered Panda/ APT 12/ IXESHE/ DYNCALC/ JOY RAT/ Etumbot

Numbered Panda targets are consistent with PRC strategic goals. In the past, it has target media outlets, high-tech companies, and government organizations. The focus of the campaign appears to be cyberespionage. It has also strategically targeted organizations involved in time-sensitive operations, such as the cleanup and containment of the Fukushima Reactor in 2011.

Numbered Panda delivers its malware through spear-phishing emails that contain binary executables concealed as screen saver files and PDF attachments. Numbered Panda bypasses egress filtering implemented to prevent unauthorized communications by dynamically calculating the C2 port by resolving a DNS. The malware uses two DNS names for communication. One name is used for command and control, while the other is used to algorithmically calculate which port it should use. One variant of the algorithm used to calculate the C2 port is to multiply the first two octets of the IP address and add the third octet to that value. This is typically represented as: (A * B) + C. For example, common values might be 200.2.43.X, which would result in communication on port 443. The group often uses blog and WordPress sites in its C2 infrastructure to make traffic seem legitimate.

Though its tools, tactics, and techniques evolve, especially after public exposure, Numbered Panda has been known to use the Etumbot exploit kit. The group has used the Etumbot, RIPTIDE, HIGHTIDE, THREEBYTE, and WATERSPOUT backdoors. Backdoors were dropped from malicious documents that exploited CVE-2012-0158 and relied on the "Tran Duy Linh" exploit kit. RIPTIDE was used from October 2012 to May 2014. The backdoor communicates via HTTP to a hardcoded C2 server, and it is proxy-aware. Its first communication fetches an encryption RC4 key that is used to encrypt further communications.

HIGHTIDE is a similar backdoor that appeared in a malicious Microsoft Word document in an August 2014 email sent from a compromised account in a Taiwanese government ministry to another official. The malware changes the user agent and the format and structure of the HTTP Uniform Resource Identifier (URI) from the RIPTIDE variant.

The THREEBYTE and WATERSPOUT malwares also surfaced in August 2014 in a malicious Word document attached to a spear-phishing email to a technology company in Taiwan. The backdoors appear to be variants of HIGHTIDE.

Hidden Lynx / Aurora

Hidden Lynx is a 50-100 member Chinese professional "hackers for hire" group that has conducted hundreds of attacks against government organizations, the financial sector, and the education sector since 2009.Within the financial sector, investment banks and asset management agencies are the primary targets. The group has also targeted stock trading firms and conducted indirect attacks on organizations that supply hardware, secure network communications, and specific services to the financial sector. Overall, the targets share the characteristics of possessing valuable information such as confidential financial data, specific knowledge of potential mergers or acquisitions, or other information that could give the client of the attacker a competitive advantage in the sector or specific knowledge of ongoing negotiations or business deals. Microsoft claims that during Operation Aurora Hidden Lynx targeted databases containing court order emails. Over half of Hidden Lynx attacks target United States organizations, while another quarter of the attacks target organizations in Taiwan or China. The broad range of targets and specificity of the information targeted suggests the mercenary nature of the attacker. The information stolen is not used for direct financial gain, so it is possible that Hidden Lynx steals information on behalf of a third party.

Most attacks begin as a watering hole attack or a spear phishing email; however, Hidden Lynx has also been known to attack public facing infrastructure or hack the supply chain in order to distribute their malware. The majority of Hidden Lynx attacks originate from C2 infrastructure located in China. Victim systems are infected with two Trojans, a mass exploitation Trojan (Trojan Moudoor) and a targeted Trojan (Trojan Naid). Each Trojan may be managed by a different division of the team. Trojan Moudoor deploys the Moudoor backdoor, which is a modified version of the "Gh0st RAT" malware. The remote access Trojan is used to control machines in significant campaigns against multiple large companies across several sectors. The Moudoor team must be sizable because the attack vector requires attackers to breach individual targets and to extract valuable and specific data from compromised networks. Trojan Naid is used in limited attacks against valuable targets. Given its restricted use and the sophistication of its application, the team behind it is likely a specialized subgroup operations team within the adversarial organization. Hidden Lynx has also used the Gresim backdoor, the Fexel backdoor, the Hikit backdoor, and the Derusbi malware in their exploit kit.

Hidden Lynx adversary regularly exploits zero-day vulnerabilities, which are purchased, discovered, or reworked from other groups' attacks. Ultimately, the adversary is methodical and it tailors its exploit kit in each attack to its victim. Hidden Lynx adapts and it develops custom tools or new techniques as necessary.

Overt Spy Structure

The overt espionage directives of the CCP pass from the party through the Politburo Standing Committee (PSC) to the State Council. The PSC consists of five to nine (currently seven) members who lead the CCP. It decides on major issues and policies when the Politburo is not in session. Effectively, the PSC is the strongest decision making body in China and its rulings *de facto* have the force of law. The State Council, consisting of (currently) 35 members, including, the Premier and heads of each governmental department, is the chief authority of the PRC. Depending on the situation, the PSC or State Council pass instructions to either the United Front Work Department, which exerts influence over Chinese nationals, or the Overseas Chinese Affairs Office, which exerts control over Chinese nationals. The United Front Department or Overseas Chinese Affairs Office further relays instructions to various communities within their respective domains.

United Front Department

The United Front Department (UFD) manages relations with non-Communist Party elite inside and outside of China to ensure that they abide by the laws set by the Communist Party. The UFD expands the sphere of influence of the Communist Party by creating strong ties with tongs and hometown associations in foreign nations, along with community leaders and, in some cases, triads and street gangs. Bonds are often formed through the exchange of position, informal trade agreements, or other incentives for influence.

Overseas Chinese Affairs Office

The Overseas Chinese Affairs Office of the State Council is the division of the PRC tasked with liaising with external Chinese communities and returning nationals. Essentially, the Overseas Chinese Affairs Office manages the circles of influence formed by the United Front Department.

Consulates and Embassies

Communications between the United Front Department or Overseas Chinese Affairs Office and external communities is facilitated by Chinese Consulates and Embassies.

Tongs and Hometown Associations

A surprising number of influential Chinese community members as well as the leaders of Tongs and homeowner associations act as local representatives of the CCP. These members pass directions, recruit members, and collect information within their area, of relevance to the CCP. Tongs and homeowner associations can be leveraged to exert pressure or pass on threats to members of the local Chinese communities to turn individuals into insider threats in their workplace or research institution.

Triads and Street Gangs

At the lowest level, triads and street gangs act as informants, muscle, and smugglers for the CCP and its operatives. The CCP has used triads and street gangs to disrupt protests, agitate dissidents, or disrupt the moral fabric of target regions by importing synthetic drugs and weapons.

Chinese Student and Scholars Associations

American universities accept a significant number of international students for a vast multitude of reasons. Some universities globally attract the most promising students, regardless of nationality. Other schools seek to diversify their student base in order to offer a balanced and realistic worldview. Realistically, many American universities target international audiences in anticipation of higher profits. For instance, in the 2013-2014 academic year, over sixty percent of Chinese students enrolled at American universities (or organizations sponsoring Chinese students) paid the full tuition cost of enrollment. This contributed an estimated $22 billion to the U.S. economy in 2014. Some schools even captured additional profit by charging international students additional fees. The overall margin of profit can be significant when compared to the often-subsidized tuition rate offered to domestic students. The excess profits allow universities, especially private institutions that do not receive government funding, to afford their programs and to offer additional scholarships to domestic students. In some cases, these short-term profits may have long-term repercussions. Among other issues discussed later in this section, International students are less likely to remain in the area around the university to benefit the community or nation, and they are less likely to donate back to the institution after graduation. Additionally, Chinese professionals trained in the United States, are returning to China with their accumulated knowledge and using it to improve China's infrastructure, economy, and education system.

According to the Institute of International Education's Project Atlas, approximately 974,926 international students were enrolled in American Universities in the 2014-2015 academic year. Approximately 31.2% of the international student population (~304,040) originated from China. This is a fivefold increase over the 62,523 Chinese students enrolled in American universities in 2004-2005. In fact, 2015 was the sixth year in a row that China was the leading place of origin for international students in the United States. U.S. Assistant Secretary of State for Educational and Cultural Affairs Evan Ryan attributes the trend to a growing middle class in China, the excellence of the American higher education system, and China's desire to be competitive in the 21st Century.

The mutually symbiotic relationship between American Universities and Chinese students is not without problems. At even a basic level, the demand for overseas education caused a "cottage industry of businesses" in China that assist in the preparation of students' applications. The poorly regulated industry is a hotbed for academic fraud and corruption. According to one educational consulting company, almost 90% of applicants submitted fake recommendations, 70% had others write their English entry essays, 50% forged high school transcripts, and 10% listed academic awards and achievements that they did not receive.

Currently, the number of resident Chinese undergraduate and graduate student populations are roughly equal. This indicates that in recent years, Chinese students have begun to enroll in American institutions directly after finishing high school, instead of obtaining an undergraduate degree from a domestic institution first. These students typically attended an international high school in China to improve their English and to prepare for American tests, such as the SAT, rather than preparing for domestic examinations. Due to culture differences and language barriers, Chinese students do not always integrate well into U.S. campus and social life. College administrators and students recognized a tendency for Chinese students, more than other international populations, to socialize primarily within their cultural community rather than engaging with the broader academic community. Consequently, Chinese Student and Scholar Associations (CSSAs) are increasingly active at over 150 universities in the United States.

Officially, CSSAs help native Chinese students balance their life, work, studies, and other issues while they are enrolled in foreign institutions such as overseas universities. CSSAs were created to bridge the cultural gap between Chinese and foreign cultures at these institutions. CSSAs may also be a pivotal overt espionage platform for the Chinese government.

The vast majority of CSSAs receive funding from the Chinese government or have an active liaison via the consulate back to the CCP. CSSA may be used to persuade students to act as temporary or prolonged intelligence assets. It is speculated that for one of these reasons, Columbia University disbanded its CSSA in March 2015 after “ongoing violations of multiple financial and student organizational policies.” Through CSSAs, students can be manipulated into passing intellectual property or research back to their home state or planting malware on a university system. How many students, conditioned from birth not to question their government, would resist the order to plug a malicious USB into a research network if their liaison threatened to revoke their funding or permission to study abroad? University networks are intentionally open and research machines are not configured with security as a priority. Compromise of a research network can enable Chinese APTs, such as Unit 61398, to leapfrog onto affiliated military or government networks.

Of the global international student population surveyed by the Institute of International Education in 2014, over 65% were pursuing degrees in Business and Management, Engineering, Natural Sciences, or Mathematics and Computer Sciences. Assuming that the percentage holds true for the Chinese population, then in 2015, over 195,000 Chinese students may have had access to research materials that directly aligned with China's Five-Year Plan.

According to a 2011 FBI report, universities are the ideal place to "to find recruits, propose and nurture ideas, learn and even steal research data, or place trainees," because young students' minds are open to suggestion and young adults are still learning how to handle responsibility, operate independently, and solve problems. While American intelligence organizations recruit using money, ideology, coercion or ego (MICE), Chinese intelligence recruit using promises of fame, feelings of lust or anger, and short term profits (FLAP). In one instance described in the report, a naïve researcher was invited to submit a paper to an international conference, after which the host requested a copy, and passed her a thumb drive. The drive downloaded every file on her laptop. In another instance, a researcher arranged for researchers in their home country to visit and allowed them to photograph lab equipment so that it could be reconstructed in their own lab. The utility of students as intelligence assets, while not flawless, should not be dismissed.

While students may not seem the best intelligence assets, China has the advantage of sheer numbers. Though the approach may seem sloppy or unprofessional, relying on human resources to obfuscate malicious activity has the advantage of overwhelming American intelligence agencies' attempts to track suspicious activities. The downside of this intelligence collection by numbers model is that assets are unreliable or untrained so agents may send multiple students after the same information and may receive the same document multiple times as a result. This increases operational risk and noise. America is not alone in this threat. In April 2014, the Sydney Morning Herald revealed the presence of a Chinese spy network in Australian education institutions and reported that Australian law enforcement agencies could not properly monitor the number of potential Chinese spies.

China collects intelligence through an application of the mosaic theory; the idea that thousands or millions of small pieces of information come together into a larger picture. The "human machine" that generates the mosaic does not even have to be entirely organized or controlled by the Chinese government. China has developed its culture and economy such that there are strong incentives for spying. Operationally, the model treats students as grains of sand. Key individuals within the multitude complete small, often seemingly insignificant tasks at the behest of an intelligence official. Why have a single spy steal 1000 documents when 1000 spies could each steal a single document? In the words of former FBI official David Major, "If it wanted to steal a beach, Russia would send a forklift. China would send a thousand people who would pick up a grain of sand at a time." In many cases, the student may never realize the harm or their utility to their government. Holistically, only a fraction of the populace are ever active assets, yet their collective actions culminate in significant gains in intelligence and intellectual property.

Unlike traditional intelligence organizations, China does not train its potential agents in any form of tradecraft. Instead, their strategy is to have the pawn lie if they are caught. The theory behind this approach is that each student's actions are of minimal risk to the Chinese government. A minority of those chosen to gather intelligence abroad may be groomed to fulfill their roles prior to leaving the country. This process ranges from reminders to remain loyal to China to regular reports of useful information to an active aggressive insider threat. Those groomed and the unwitting assets can be further compelled to pass more information to their handlers through threats, guilt, or a sense of national pride. In addition to collecting information, student spies may be used by CSSAs to welcome visiting leaders at airports or to block protest groups from sight.

Chinese students may also be used to coerce or recruit domestic students. University students rarely consider national security when they share notes and research materials. In April 2015, the FBI warned U.S. students travelling abroad to guard themselves against attempts to influence their behavior or recruit them as spies. Chinese intelligence agents target students who study abroad because they are prime candidates for positions in governments and large companies. These "seeding operations" attempt to grow study abroad students into potent insider threats. In a podcast, Mollie Halpern, at the FBI Office of Public Affairs, noted: "To foster the relationship, foreign intelligence operatives will flatter and encourage students, show interest in their future success, and even promise to help them obtain a government-issued visa or work permit—but it's all disingenuous and empty promises. The truth is, the operatives are just using the student as a pawn to achieve their own ends, without concern for the student's welfare or future."

This warning was accompanied by a video featuring the story of Glenn Duffie Shriver. Shriver was an American student who answered a $120 ad in 2004 to write a paper on U.S.-China relations. Through a series of connections, Shriver was financially coerced into spying on the United States for China. Over the next few years, the Chinese intelligence agents paid Shriver over $70,000 to attempt to pass examinations to enter the United States Foreign Service and the CIA. In June 2010, Shriver was arrested and charged with "making false statements", for failing to reveal his associations during his application to the CIA, and for "willingly conspiring to provide national defense information to intelligence officers of the PRC." In October 2010, as part of a plea bargain, Shriver pled guilty to one count of conspiracy to commit unlawful conveyance of national defense information. In January 2011, he was sentenced to four years in prison, though he was released in late 2013. According to the department of Justice, between March 2008 and October 2010, 45 individuals were convicted in 26 cases involving espionage on behalf of China, though Shriver was the only student among them.

In May 2016, growing concerns over the threat of espionage in critical research environments resulted in the State Department proposing a rule that would bar foreign students from certain research projects and classes involving information seen as vital to national security. Of particular concern was research related to defense technologies, energy engineering, and aerospace applications. The Association of American Universities, representing 62 leading research institutions including Harvard, Duke University, and the University of Chicago, as well as Stanford University, Massachusetts Institute of Technology

(MIT) and the University of Pennsylvania have criticized the rule, citing “disastrous consequences.”

Academic Solicitation

As was the case with Glenn Duffie Shriver, some foreign powers attempt to solicit academics through seemingly innocuous proposals or offers of collaboration. In some cases, such as with Shriver, these are active attempts to start a dialogue and build a relationship that will increase the leverage over a target asset until they are malleable. In other instances, academic solicitation is a covert attempt to obtain classified or proprietary information through requests to review academic papers or host lectures. The innovation or insight contained in an un-vetted presentation or publication can be critical to military and strategic operations. For example, in 1998, Chen Dingchang, a head of a Chinese military-sponsored research group on anti-satellite technology, viewed a presentation at the University of Florida about diamond-coating manufacturing. The technology could also be used in missile seekers and other systems. In 1999, Chen and other authors published a report in a Chinese journal that credited the Florida presentation in assisting them in overcoming a technical bottleneck in China’s development of anti-satellite warheads.

According to a 2011 U.S. Defense Department report, “Placing academics at U.S. research institutions under the guise of legitimate research offers access to developing U.S. technologies and cutting-edge research” in such areas as information systems, lasers, aeronautics and underwater robots. The report further stated that these attempts increased eightfold between 2009 to 2010. In other cases, professors may receive a request to collaborate, but they may not be fully aware of the allegiances of the requester. Academia is an open, collaborative field that is built upon the nurturing of ideas amongst distant and far-flung individuals at universities around the globe. Researchers, especially in niche fields, may not suspect an interested party of malice; instead, they may revel in the sudden interest in their work. For example, several years ago, Professor Daniel J. Scheeres, a frequent host of visiting scholars, received a request from Yu Xiaohong to study with him at the University of Michigan. Xiaohong cited an affiliation to the civilian Chinese Academy of Sciences and she expressed “general interest” in Scheeres research into the movement of celestial bodies. When Yu arrived, her questions made Scheeres uncomfortable. Specifically, he was disconcerted by her interest in military satellite-orbit applications of the field. He did not deeply engage with Xiaohong and he later stopped accepting visiting scholars from China altogether as a result of the experience. He was unaware at the time that Xiaohong listed her address as the same as the Academy of Equipment Command and Technology, where Chinese military cadets and officers are trained, or that she had previously co-authored an article on improving the precision of anti-satellite weapons. Yu Xiaohong later wrote a paper about the implications for space warfare of the NASA Deep Impact mission, which sent a spacecraft to collide with a comet.

Front Companies

As of 2010, China had over 3200 front companies in the United States whose sole purpose was to acquire American technology. That number has likely increased significantly within recent years. In 2011, U.S. and Canadian universities earned $2.5 billion from licensing technology. Given that universities do not tend to investigate companies before licensing software and inventions, some of the licenses may have been issued to front companies for China and other foreign powers. Efforts to detect front companies have improved through the collaboration of some academic institutions with the FBI and other law enforcement; however, many universities resist such a connection out of fear that it will hamper research and intellectual freedoms or establish an undesired precedent.

Insider Threats

Chinese researchers trained at American universities can be leveraged by CSSAs, tongs, or even triads, to act as insider threats at the employment that they obtain through the University's network. For example, Hanjuan Jin joined Motorola Solutions Inc. as a software engineer shortly after earning a master's degree from University of Notre Dame in South Bend, Indiana. While at Motorola, she received a second master's degree in computer science from the Illinois Institute of Technology in Chicago. Despite the opportunities offered by a bountiful education, in February 2014, Hanjuan Jin, was found guilty of stealing trade secrets, although she was acquitted of charges that she did so to benefit China's military. Hanjaun Jin allowed the CCP to influence her life years after graduation, despite living comfortably in the United States.

Some Chinese nationals were groomed to be international insider threats at foreign organizations. Others are threatened, bribed, or otherwise coerced into passing information or compromising systems on behalf of the CCP. The insider's contribution could be as little as clicking on a spear phishing email, plugging in a USB, or distracting an employee from their system.

Monitored Communities

The Chinese university network of students or placed government officials are not limited to the theft of intellectual property and research. They also monitor those critical of the Chinese regime. Students, professors, and others critical of the Chinese Communist Party have reported interrogations, and in some cases threats, when visiting China in response to comments that they made thousands of miles away from Chinese shores. Tongs, triads, and gangs can also be used in a similar capacity in Chinese communities. One Australian lecturer was interrogated four times in response to his criticisms. Joshua Philipp of Epoch Times reported, "Chen Yonglin, a former Chinese diplomat at the Chinese Consulate in Sydney, told Epoch Times when he defected in 2005 there were more than 1,000 Chinese secret agents operating in Australia, alone." Similarly, in an article for Business Insider, Jack Murphy recounts his awkward experience of naively asking a study group of himself and three Chinese students at Columbia University about the practice of Falun Gong. He recalls the palpable silence and fear imposed by what he thought was an innocent question and his experience discovering that he had unwittingly pitted his groupmates in a prisoner's dilemma if they answered him. Jack learned that much as CSSAs, Tongs, and Triads can be leveraged to monitor Chinese nationals, so could communities of Chinese students be used to monitor each other for signs of subversion of the PRC. Within its borders, the CCP uses the Great Firewall and signal intelligence to control and monitor the online activities of its people. Outside of its territory, the CCP relies on overt spy organizations to monitor potential dissidents and there are actually allegations that the one of the departments collects covert and overt intelligence for the sole purpose of informing an application that monitors the opinions and activities of every Chinese citizen, domestic and abroad. This constant state of observation has induced a chilling effect in Chinese citizens, which prevents many from consciously subverting the CCP.

One sophisticated monitoring system, referred to as the Social Credit System (SCS) will go into full effect by 2020. The SCS will make Orwell's Big Brother seem distant by comparison. The SCS attributes a rating to each citizen based on constant appraisals of their physical and virtual activities, their dialogues, their patriotism, their purchase habits, their friends' opinions of them, and numerous other characteristics. If ever a citizen acts outside predetermined parameters, then their score lowers in the system. Those with high scores receive tangible benefits, such as travel visas, access to business loans, and other incentives while those with low scores receive punishment from the government as well as active disincentives. Much like Orwell's dystopia, the system rewards those who report "breaches of trust." One example of a disincentive is that those who score low may become social pariahs because the SCS actively punishes those with a higher score from associating with those below them. Currently, methods of developing SCS scores are being tested at eight companies under state-approved pilot programs. One such pilot focuses on 400 million users of the Alibaba network to develop scores based on financial information and purchasing habits. While the algorithm is fine-tuned, China is implementing the infrastructure to make the Social Credit System feasible within the mainland. Moreover, external communities may not be exempt from monitoring.

In September 2015, Joshua Philipp of Epoch Times reported that Lenovo, Huawei, Xiaomi, and other devices manufactured in China had preinstalled spyware that allowed Chinese companies to track users, listen to calls, and make online purchases. Worse yet, many of the products manufactured in China already feature language in the terms and conditions authorizing the Chinese government to monitor the data that passes through the devices (even those located in the United States) for indicators of subversion against the CCP. By using the devices, the users unwittingly agree to abide by the laws and authority of the Chinese Communist Party. Moreover, many companies that operate in China are already subject to rigid compliance regulations, such as the inclusion of a CCP liaison and in some cases, backdoors into hardware and software. Currently, every company operating within Chinese borders with more than 50 employees are required to have at least one liaison to the Communist Party on site. For example, Joshua Philip of Epoch Times explains, "At Mitsubishi Electric (Guangzhou) Compressor Co., Ltd., the number of CPC members exceeds

100, and nearly half of the managers above the team leader level are CPC members at the Japanese company." He adds, "Chen Kailong with the Party School of the CPC Central Committee said foreign companies are increasingly supportive of establishing Party branches because they help with the enforcement of Chinese laws and regulations and mediation in labor disputes." These liaisons can internally influence the organization or act as insider threats.

China's new cybersecurity law proposes even greater censorship and control over companies. Under the guise of added security for its people, the CCP may require any company that operates in China to allow the Chinese government unrestricted access to their systems and control over their internet access. In effect, the CCP could install backdoors and spyware in every device that passes through China. Even if foreign citizens somehow manage to avoid purchasing devices manufactured in China, their lives may be monitored through numerous public IoT devices of which China is the sole manufacturer. This global espionage platform can be combined with the dossiers and databases constructed from the information exfiltrated in the incessant cyberattacks conducted by Chinese APTs, to gain unparalleled advantage over the global population.

Conclusion

ICIT research rarely fills pages with artistically designed info graphics, charts or graphs. Instead we compose our reports with raw, interlinking linguistic tiles with a 12-point font and single spaces. Our research is meant to shed light and inform rather than impress and offer silver bullet solutions. For the past year, this particular report has been heavily requested by federal agencies, members of Congress, journalists and private sector organizations that have been profoundly affected by Chinese intellectual property theft. With such a high stakes topic about a state adversary that has had such a devastating impact on industry, economy and National security, we found it necessary to pay less attention to softball language and zero in on the facts and realities of this particularly devious antagonist.

This report was not about China's grotesque human rights violations, their poor manufacturing quality, fifty cent trolling army propaganda or continuous feuds between their military and government. And this report was not about the latest conversations of byte for byte retaliation by industry against Chinese actors with weaponized data and cyber-attack. This report is about the layers of espionage and theft and those malicious actors who carry out these overt and covert attacks on Western industry. Uncovering the layers and pinpointing the contributors and liberating this document into public discussion are the first steps in understanding a complicated adversary with the intent on combatting its initiatives.

Combatting the complicated layers of China's multipronged attack means erecting profound layers of cyber and physical security composed of bleeding edge technology and the latest in counter intelligence expertise. True multinational threat sharing between industry and law enforcement compounded by a judicial system that combats insider threats and IP theft with harsh penalties will pave the way for the legislative community to bring forth a new standard in international cooperation to combat the Chinese menace.

Contact Information

Legislative & Executive Branch Inquiries:

- James Scott, Senior Fellow, ICIT (james@icitech.org, 202-774-0848)

Federal Agency Inquiries:

- Parham Eftekhari, Senior Fellow, ICIT (parham@icitech.org, 773-517-8534)

Links

Website: www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg

Sources:

The Atlantic:

http://www.theatlantic.com/education/archive/2015/05/american-universities-are-addicted-to-chinese-students/394517/

America Enterprise Institute:

https://www.aei.org/publication/chinese-economic-espionage-mixed-signals-at-years-end/

BBC:

http://www.bbc.com/news/world-asia-china-34592186

Bloomberg:

http://www.bloomberg.com/news/articles/2012-04-08/american-universities-infected-by-foreign-spies-detected-by-fbi

Business Insider:

http://mobile.businessinsider.com/chinese-student-spies-2015-8

Chinese in the U.S.:

http://www.chineseinus.com/cssa_list.htm

CNBC:

http://www.cnbc.com/2015/09/25/us-china-agree-to-not-conduct-cybertheft-of-intellectual-property-white-house.html

CrowdStrike:

http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

http://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem

https://www.crowdstrike.com/blog/whois-anchor-panda/

https://www.crowdstrike.com/blog/whois-numbered-panda/

Dark Reading:

http://www.darkreading.com/endpoint/chinese-cyberspies-pivot-to-russia-in-wake-of-obama-xi-pact/d/d-id/1324242?

http://www.darkreading.com/attacks-and-breaches/crowdstrike-falcon-traces-attacks-back-to-hackers/d/d-id/1110402

Data-Informed:

http://data-informed.com/china-social-credit-system-a-frightening-use-of-big-data/

The Diplomat:

http://thediplomat.com/2015/09/remember-chinas-announced-300000-troop-cut-not-everyones-happy-about-it/

Epoch Times:

http://www.theepochtimes.com/n3/968736-chinese-student-spies-overwhelm-us/

http://www.theepochtimes.com/n3/1094262-chinas-silent-war-on-the-us/

http://www.theepochtimes.com/n3/1748900-spy-software-found-pre-installed-on-lenovo-huawei-and-xiaomi-smartphones/

F-Secure:

https://www.f-secure.com/v-descs/backdoor_w32_poisonivy.shtml

FBI:

https://www.fbi.gov/about-us/investigate/counterintelligence/higher-education-and-national-security#disablemobile

FireEye:

https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html

https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html

https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

Forbes:

http://www.forbes.com/sites/jnylander/2015/03/25/columbia-university-closes-chinese-student-organisation/#559748c24f4d

Foreign Policy:

http://foreignpolicy.com/2015/11/16/china-us-colleges-education-chinese-students-university/

The Hacker News:

http://thehackernews.com/2015/03/china-cyber-army.html

Homeland Security Today:

http://www.hstoday.us/single-article/china-based-adversaries-pose-major-cyber-threat-in-2016/a9252680701e315c9b06f1762be9b7a2.html

ICIT:

http://icitech.org/know-your-enemies-2-0/

Institute of International Education:

http://www.iie.org/Services/Project-Atlas/United-States/International-Students-In-US#.V3sxoaKo0jc

http://www.iie.org/Who-We-Are/News-and-Events/Press-Center/Press-Releases/2014/2014-11-17-Open-Doors-Data#.V3szrqKo0jc

Kaspersky Labs:

https://securelist.com/blog/research/35936/nettraveler-is-running-red-star-apt-attacks-compromise-high-profile-victims/

LA Times:

http://www.latimes.com/world/asia/la-fg-china-us-student-spying-20140507-story.html

Listverse:

http://listverse.com/2016/02/05/10-ways-china-might-be-spying-on-you/

The New York Times:

http://www.nytimes.com/2014/06/10/technology/private-report-further-details-chinese-cyberattacks.html?_r=0

Palo Alto Networks:

http://researchcenter.paloaltonetworks.com/2015/07/ups-observations-on-cve-2015-3113-prior-zero-days-and-the-pirpi-payload/

Reuters:

http://www.reuters.com/article/us-cybercrime-usa-china-idUSKCN0J42M520141120

http://mobile.reuters.com/article/idUSKCN0WG2L5

http://news.trust.org/item/20160520140331-0ui5x/

http://www.reuters.com/article/us-college-cheating-iowa-special-report-idUSKCN0YG2T5 http://mobile.reuters.com/article/idUSKCN0YB1QT

http://www.reuters.com/article/us-china-cyber-lawmaking-idUSKCN0ZD1E4

Symantec:

https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=26611

The Sydney Morning Herald:

http://www.smh.com.au/national/chinese-spies-keep-eye-on-leading-universities-20140420-36yww.html

Threatpost:

https://threatpost.com/naikon-apt-group-tied-to-chinas-pla-unit-78020/114798/

Trend Micro:

http://blog.trendmicro.com/trendlabs-security-intelligence/evilgrab-malware-family-used-in-targeted-attacks-in-asia/

http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/112/pulling-the-plug-on-plugx

The United States Patent and Trademark Office:

http://www.uspto.gov/sites/default/files/news/publications/IP_Report_March_2012.pdf.

The Wall Street Journal:

http://www.wsj.com/articles/heavy-recruitment-of-chinese-students-sows-discord-on-u-s-campuses-1458224413

The Washington Post:

http://voices.washingtonpost.com/spy-talk/2010/07/cia_applicants_arrest_tops_wav.html