Crouching Tiger, Hidden Dragon, Stolen Data

Context Information Security
whitepapers@contextis.com

March 2012

Contents

Executive Summary

Media reports show that targeted cyber attacks against government and commerce have been ongoing since at least 2003 and possibly some time before that. By far the largest sponsor of these attacks is the Chinese state. This is not a new problem; it is espionage with a different methodology.

These attacks are far from random or indiscriminate. These attacks are designed to steal information that will fulfil a clear set of requirements set by the Chinese state and furnish them with political, commercial and security/intelligence information. These requirements are carefully and clearly identified, shared with a number of government departments and constantly updated. There is evidence of worldwide targeting but only a minority of attacks are identified and fewer still made public.

This is a structured program and the main protagonists in China are widely believed to be the Third Department of the People's Liberation Army. Even using conservative estimates it is likely that the program employs thousands of military personnel. While the military program may be the most developed and sophisticated, it is likely that other parts of the Chinese state and even the private sector may also be carrying out similar attacks.

There are clues to the companies and types of data most at risk. In particular the Five Year Plan[1] and the National Outline for Medium and Long Term S&T Development[2] give detail on the areas in which China intends to excel and identifies specific technology which the Chinese want to develop or otherwise acquire. Electronics, telecoms, manufacturing, extraction, energy, biotech, pharmaceuticals, aerospace, space and defence are sectors at the highest risk, alongside companies and services such as law and accountancy firms that support them and hold their data.

The likely recipients of stolen commercial data are the 117 Chinese State Owned Enterprises that dominate the economy. These companies are closely linked to the state and the Communist Party which has power over strategy, senior management and even wages. Companies with SOE competitors should be especially concerned about data security.

Two factors make western governments and companies more vulnerable to Chinese targeted cyber attacks. Firstly, there is reluctance for governments and companies to accuse China directly or take any form of action for fear of either being isolated politically or being blocked from a lucrative developing market. Secondly, a long term reliance on traditional security products such as anti-virus, coupled with a lack of education about the threat, leaves businesses vulnerable to attack and unprepared for any investigations that are required in the aftermath of a compromise.

Context has extensive experience of detecting and investigating targeted attacks and working with clients to help protect their data.

[1] Chinese Government Official Web Portal website

[2] China International Science and Technology Cooperation website

Introduction

There have been many media reports in recent years about cyber attacks on governments and a variety of private sector companies. The rather ambiguous term 'Advanced Persistent Threat'[3] ('APT') is widely used to describe any attack that appears to have compromised computers in these companies or organisations, regardless of the source or purpose of the attack. We prefer simply to call them 'targeted attacks' and leave marketing terms to one side. This paper is not concerned with the technical aspects of targeted attacks, it seeks instead to inform readers about the full scope and nature of these attacks, the reasons why they are launched and the people and policies behind their design and execution.

Many reports of attacks inevitably end by asking 'who did it?' But the answer is rarely straightforward. Western Governments usually allege the attacks come from 'Asia' or the 'Far East', rather than risk offending the Chinese government. Large corporations are similarly vague in their descriptions of these events, for fear of harming lucrative business arrangements. Security 'experts' always caution that IP addresses can be used as hop points through which attackers disguise their true origins, so perhaps this could be a case of other countries trying to make it look as if China was the source. While this is true, if something looks, walks and quacks like a duck, it is almost always a duck.

We will not be so coy. This paper will look directly at the most prolific sponsor of computer network exploitation attacks: China. We know other countries have implemented similar programs for attacking computer networks and have seen many examples of these in our work over the last few years, but our focus here is China.

We will examine various aspects of these attacks, including the nature of the information targeted and the types of organisations threatened. We will consider the effort involved in planning, executing and managing these attacks; and assess the information products they generate, in order to understand the scale of human involvement and the government policies that sponsor information theft via targeted attacks. With all this in mind we will then postulate on where the stolen information goes and how it may be used.

[3] Advanced Persistent Threat has recently become a catch all term for targeted attacks against computer networks and is often used to describe the malware. In fact, the term was first coined by the United States Air Force in 2006, specifically to refer to China – without actually saying China. 'Advanced' because the attackers could use a variety of attacks to get access to a network and could raise their game to use zero day vulnerabilities if necessary; 'Persistent' because the attacks would not stop until the attacker had achieved their objectives; and 'Threat' because this attack was not automated like a botnet, but was conducted by humans who adapt and evolve their methods to evade defences.

Categorising Attacks

Many commentators have divided the targets of attacks into four categories: political, economic, technical and military. This works as a general model, but focuses on the target of the attack as a whole rather than considering the type of information the attacker seeks to steal. If a criminal gang unleashes a phishing attack aimed at harvesting banking credentials and it is the employees of a butchers shop and a bakery that fall victim to it, that does not mean the attack was targeting bread and meat.

Bearing this in mind, we divide target areas into the following categories:

- Political. The information targeted will inform the state on the political positions of other governments on a range of issues, including economics, trade and human rights. Typical targets are government departments, embassies, trade bodies, NGOs, and international political groups such as the UN, G20, World Bank and IMF.
- Commercial. The information targeted will be of value to the private sector within that country (even if the lines between private and public sectors are blurred). It may include IPR, product designs, negotiating positions for sales discussions, mergers and acquisitions information and strategic plans (particularly in relation to the attacking country).
- Intelligence. The information targeted here will be used to safeguard internal security by the attacker country (this may entail intimidation or close monitoring of minority or opposition groups or individuals) and to enable analysis of the military technology, capabilities and intentions of other countries.

There are a number of major problems that need to be overcome when seeking a complete understanding of the scale and purpose of attacks. Many will never be detected, those that are may not always be reported; and the vast majority are not investigated by professionals with a good understanding of these types of attack. Dealing with the technical aspects of the compromise alone is not enough: the victim needs to know why they were being attacked, by whom, what data was stolen and where it may go.

While government agencies, such as the Centre for the Protection of National Infrastructure[4] (CPNI) in the UK and the FBI5 in the US, are working successfully with larger organisations to identify potential threats, reduce the risk of successful attacks and in some cases to identify and investigate specific compromises, this assistance is not available to every company. It is not generally available to those that need it the most – companies that innovate and excel in niche areas and supply technology or products that other companies make use of in larger projects. These companies live and die by the success of their research and development, but often lack the budgetary resources or expertise required to adequately protect their networks from this type of threat.

Even when compromises are investigated by companies that understand the attackers and their motives, it is often not felt to be in the interests of either party to publish the findings of those investigations, or to share the results with the affected company's competitors, who

[4] http://www.cpni.gov.uk

[5] http://www.fbi.gov/

may be suffering from similar attacks. There is also a widespread lack of understanding of targeted attacks among IT staff, a lack of dedicated IT security personnel and, sometimes as a consequence of IT functions being outsourced, an over-reliance on traditional security products such as anti-virus and firewalls – both of which are ineffective against even lower end targeted attacks. The pressure exerted on IT staff from the business is primarily concerned with service uptime and availability rather than security; and budgets for even routine security operations such as penetration testing are under constant pressure. It is a sad fact that, for many businesses, money for IT security only becomes available once a serious problem has been identified, by which time it is often too late.

One more common problem in private sector companies is that some managers take the attitude that they would prefer not to know about security problems. Information Technology departments may worry that commissioning a detection exercise to find compromised hosts in their environment, could reveal a series of attacks and the theft of data, which might not be good for their career prospects. Higher up the management chain, board members may even choose not to spend money on security on the grounds that this will affect profitability and perhaps the size of their salaries or bonuses. They may instead prefer to postpone any major spending on security until they absolutely have to.

Why Cyber?

Clearly, the Chinese government is keen to understand the political decisions taken by other countries and the activities of opposition groups within China, so it is hardly surprising that it orchestrates the compromise of computers via emailed Trojan attachments or links to compromised websites on a large scale. This is nothing new; just traditional espionage with a new methodology.

Until recently China, like most other developed countries, would have hand-picked intelligence officers from universities and the military, trained them in the arts of developing relationships, recruiting agents and how to covertly gather information to pass back to Beijing. They would have been deployed to embassies overseas or under a business cover.

The arrival of the Internet did not sound the death knell for human spying, it simply offered an attractive alternative. Moving espionage operations into the virtual world brings some advantages. Firstly, it does not require anyone to be sent overseas. This is an important change for the governments of communist countries, naturally suspicious of the long term intentions of even their most trusted officials. It means there is less need to invest in lengthy training processes. Instead, hacking operations can be broken down into simple tasks and partly automated to minimise the need for operators with advanced technical skills. Conducting these operations is cheap and carries a lesser risk than human espionage: even if the target is fairly certain as to the origin of an attack, the sponsoring government can claim to be a victim of mistaken identity or of a western conspiracy.

But the key benefit of this type of espionage is that any piece of information stored anywhere in the world on a computer or a network connected to the Internet is only a few clicks away from being stolen. There are even attacks that are designed to jump to computers not connected to the Internet. If the prize is great enough and the attacker is determined enough, there is always a way.

How Cyber?

This paper is not concerned with ‘how’ the attacks happen, which is a subject for a white paper in its own right. Typically however, the attackers target the desktops and laptops of the victim’s organisation and send emails with an attachment containing an exploit, (often an Adobe PDF or Microsoft Office document) that is targeted at one person. Once the victim opens the attachment the exploit executes, typically downloading and automatically installing a Trojan, which the attacker can then use to access the victim’s system. The attackers also utilise website vulnerabilities which exploit vulnerabilities in web browsers such as Internet Explorer or Firefox to download malicious code onto a machine when a user clicks on a link in an email. Once the attacker has this foothold on the network, they typically look to download and use further hacking tools to escalate privileges to gain administrative access to key internal servers such as Domain Controllers or File Servers. Once achieved, the attackers typically use another remote desktop or laptop on the network to collate the data stolen and exfilitrate it to their remote servers.

In the case that a network is fully patched and constitutes a hard target, the attackers can respond and raise their game substantially. This could include exploiting a zero day vulnerability[6] or employing other means of installing an implant, such as using physical access to introduce an attack or even attacking a supply chain.

The Targets

Despite opening up greatly over the last 15 years, China is still very much run by the Communist Party. The Party has control over and involvement in every area of daily life, but despite the internal focus, China is careful to keep an eye on the outside world and how the country’s institutions and companies are perceived by foreign governments. An understanding of other countries’ political positions on key issues that affect China is key to forward planning, especially for an economy built on cheap exports.

The governments in which the Chinese state is most interested fall into three groups: its nearest neighbours: Japan, Taiwan, the disputed (semi-autonomous) Tibet, Mongolia and the Muslim ‘Stans’ to the west; other powerful states with international influence such as the US, Russia, the UK, Germany, France and India; and finally states with strong economic links to China including Brazil, Iran, Australia, parts of Africa and Southeast Asia.

Whilst China will not be interested in the entire spectrum of government affairs in each of these countries, there will be some interest in some parts of all these governments’ activities. Gathering information on this scale is a massive task: monitoring relevant issues, identifying individuals with access to that information and crafting attacks in the appropriate form and language.

The other constant preoccupation of the Chinese government is the maintenance of internal and external security. The enemies of the internal state are referred to as the ‘Five Poisons’: the separatist Uighurs (a mainly Muslim group in Northeast China), Tibetan separatists, pro-democracy supporters, supporters of an independent Taiwan and followers of the religious group Falun Gong. Keeping tabs on these groups and on their known supporters at home and overseas is another huge task. The Ministry of State Security monitors

[6] A zero day vulnerability is one which is not publicly known and for which no patch exists.

the communications between individuals and groups, a task made considerably easier through the deployment of Trojans to compromise computer equipment. As a minimum, security services would usually seek to steal email account login and password details in order to be able to log in remotely and read emails. Google has confirmed this activity was taking place on the Gmail accounts of Chinese dissidents.[7]

China wants a clear picture of other countries' military activities in order to inform its own tactical and strategic decisions. Human penetrations of foreign military organisations are extremely difficult and carry significant risks, so relatively passive email attacks are an excellent substitute activity, where no single incident can be seen as an act of aggression meriting a military response. It remains to be seen whether thousands of attacks conducted over a long period of time will come to be regarded as having been a provocative act warranting a military response.

While China has been publicly – albeit mostly not directly – accused of carrying out attacks against governments, military organisations and military contractors numerous times, there are also plenty of examples of private sector organisations being targeted. Several stand out from the last few years: the 'Aurora[8]' attacks that hit Google, Adobe, Juniper, Northrup Grumman and others; the McAfee-dubbed 'Night Dragon[9]' attacks that struck companies around the world in the energy sector; and the 'Shady RAT[10]' attacks that affected the steel industry, heavy engineering, construction and communications companies and others.

Interestingly, despite reporting on the intrusions, McAfee does not highlight the fact that anti-virus software did little to stop the attacks in the first place. In all likelihood all these various 'operations' formed part of the same attack, with different groups or military units carrying out operations sponsored by the Chinese state. One attack that was clearly carefully planned, and equally linked to the others, was that conducted against RSA[11], whereby attackers stole information which allowed them to replicate the SecurID tokens used by companies to authenticate individuals logging onto their networks from remote locations.

Armed with those stolen credentials, an attacker would be able to log in to company networks as if a real user. The full extent of this breach has not been publicly disclosed, though we do know that Lockheed Martin was attacked and we can speculate that other defence contractors were also targeted. As full details of what was stolen have never been put into the public domain, we can only guess at the targeted information. Google claimed Intellectual Property had been stolen, though no further details were given. But these companies were all targeted for a reason. Data was identified that would somehow be of use to China. We will look at who laid out the requirements for this data next.

[7] http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

[8] http://en.wikipedia.org/wiki/Operation_Aurora

[9] http://www.mcafee.com/ca/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

[10] http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

[11] http://www.rsa.com/node.aspx?id=3872

The Requirements

We should never think of Chinese cyber attacks as uncoordinated, random or indiscriminate. They target companies, governments or individuals because a specific requirement has been identified. Context has studied a number of Chinese government policies, documents and stated aspirations, as well as Chinese commercial structures, which may show why targets may have been picked; and may also help companies to gauge whether their business should consider itself to be at risk of being targeted by a Chinese attacker.

The key documents are the Five Year Plan and the National Outline for Medium and Long Term S&T Development. We will also theorise around the (unwritten) intelligence requirements. We will then later investigate China's state-owned enterprises as potential generators of requests for material to be stolen via targeted attacks; and as consumers of stolen data.

The Five Year Plan is a series of development initiatives, both social and economic, that set high level goals for where the Communist Party would like to see the country in five years' time. The latest Plan was finalised in October 2010 and applies to the period 2011 – 2015. It contains goals for urbanisation rates and targets for economic growth; details the foreign industries that will be invited to do business in China, the scale of proposed construction projects and areas of the country/economy where further development should be encouraged. These high level goals filter down to all government departments at national, regional and local level, where individual initiatives are managed. But the plan also hints at the areas where China feels it needs to concentrate its efforts, or where it needs to catch up with other countries elsewhere in the world.

However, targeted attacks are 'state sponsored', which means that it is not the government that conducts the attack, but departments of the state or affiliated groups. When the government decides that, for example, it requires intelligence relating to US military operations in Afghanistan, different parts of the state intelligence apparatus will respond to this requirement, each bringing different skill sets to bear on the problem of finding the required information. For example, the People's Liberation Army (PLA) has departments with access to satellite photography, which could provide information on troop movements. Another department may have access to Signals Intelligence (SIGINT), which intercepts communications. Chinese diplomats in the country will speak with their Afghan counterparts about the situation, while intelligence officers, perhaps in diplomatic or even non-official roles, are able to exploit human agents with access to useful reporting. To complement all of these sources, cyber attacks can be used against a variety of targets such as the Pentagon, military forces in theatre, the US embassy, defence contractors and representatives of the UN and NATO. As cyber proves its worth (if it hasn't already) other parts of the government will seek to develop their own cyber capability to add to their existing capabilities, not wishing to be outshone by competing departments.

One of the points on the Five Year Plan for instance is 'More efficient development of nuclear power under the precondition of ensured safety', which could suggest that any information gathering attacks against the nuclear energy industry (as opposed to sabotage or Stuxnet[12] style attacks) could be carried out with the express intention of supporting this part of the Plan.

The attacks could be directed against nuclear plants themselves in an attempt to obtain operating information; construction companies, to steal building plans (which may also be of value to the military in case of war); regulatory bodies for rules, policies and procedures; and any of the hundreds of companies that build parts for the plant or develop technology used in the nuclear process.

In terms of who could be carrying out the attacks, we have to consider not only the military (the Third Department of the PLA has the remit for cyber operations, though other areas are likely to have some capability too), but also nuclear construction companies, the government department with a remit for the energy industry, or any of the hacking groups that are closely affiliated to the state. Different campaigns may even be competing to steal the same information with the rewards going to the attackers who get it first.

The Plan also advocates the development of high-end manufacturing, hi-tech industry, modern agriculture, high-speed rail and hydropower. The Plan does not explain in any detail how this development will be achieved, although in some cases it does specify that certain areas will be prioritised for direct foreign investment. In these cases, foreign firms are invited to partner with local firms to complete a project and engage in 'technology transfer'. This means (officially) that the Chinese company will learn skills from the foreign company and develop their own capabilities in the area. Unofficially, it generally ends up with the foreign company having its IP and technology stolen and then finding that it no longer has an invitation to do business in the country.

One good example of technology transfer can be seen in the area of high speed railways. Originally, trains were purchased from Kawasaki, Siemens and Bombardier and these manufacturers helped create the first high speed lines which opened in 2007. Soon afterwards China started to build its own high speed trains, modelled on those imported, but with reconfigured components. There is an ongoing legal case brought by Kawasaki and other Japanese companies relating to Chinese companies attempting to patent Kawasaki technology associated with high speed rail[13]. The current Chinese patent laws specify that the owner of a patent registered in China must be Chinese and that the Chinese holder will also be favoured over any foreign claim for the same technology.

In July 2011 two high speed trains collided near Wenzhou, killing (according to state media) 40 people. There were concerns that the trains contained stolen foreign technology and it has been suggested that this is why the wreckage was buried even before the rescue operation had been completed. It has also been suggested in certain quarters that burying the wreckage stopped any investigation by the manufacturers into what went wrong (and whether or not there was stolen technology present). This action attracted widespread criticism of the government, even from some sources within China.

[12] http://www.bbc.co.uk/news/technology-11388018
[13] http://online.wsj.com/article/SB10001424052748704814204575507353221141616.html

Boosting Domestic Enterprise

If the Five Year Plan is short on detail, the National Outline for Medium and Long Term S&T Development is not. This policy essentially sets out the requirement for 'Indigenous Innovation', the areas where China should not rely on western technology, but should develop a home-grown alternative. The strong desire for domestic products stems from two issues. Firstly a suspicion that foreign technology could be used covertly in ways for which it was not originally intended it would be used (for the benefit of the attacking country). Secondly because in order to sustain high growth rates and satisfy domestic consumption it is better if China manufactures products of equal capability and sells them to its own market than it is to import goods at high prices. The plan for Indigenous Innovation drills down into each of the areas where China wants to develop a capability in some detail, even setting out priorities. The list of eleven areas comprises:

- **Energy**. Oil and gas exploration, distribution and power grids, low cost renewable energy, coal liquefaction, industrial energy efficiency
- **Water and Mineral Resources**. Distribution, conservation, desalination, zoning and development of resources
- **Environment**. Pollutant control and recycling, restoration of vulnerable ecosystems, maritime ecosystem protection, environmental change
- **Agriculture**. Genetic resource development, disease prevention, use of agro-forest biomass, multifunctional farming equipment, modern dairy industry
- **Manufacturing Industry**. Basic/generic parts/components, digital intelligent design, recycling iron and steel, marine engineering technology, engineering processes for the defence industry
- **Transportation**. Construction and maintenance technology, high speed rail, energy efficient cars, traffic control systems, alternative fuel based cars
- **Modern Service Industry**. Next generation Internet technology, high performance computers, digital media content platforms, HD displays
- **Population / Health**. Treatment of diseases, medical processes
- **Urbanisation**. Green buildings, architectural energy efficiencies
- **Public Security**. Security warning systems, bio-safety measures
- **Defence**. [Classified]

In addition to these areas, which already contain a lot of areas that targeted western companies operate in, there is a further list of 16 'Major Special Projects'. These projects are intended to add to the overall strength of China. Previous examples of such projects include the development of the hydrogen bomb, launching satellites, manned space flights and hybrid rice. They are intended also to be a source of national pride. If one can see the potential for cyber attack to enhance many of the areas outlined above, the list below gives even more scope for the targeted theft of data from companies and governments around the world:

- Core electronic components, high-end general use chips and basic software products
- Large-scale integrated circuit manufacturing equipment and techniques

- New generation broadband wireless mobile communication networks
- Advanced numeric-controlled machinery and basic manufacturing technology
- Large-scale oil and gas exploration
- Large advanced nuclear reactors
- Water pollution control and treatment
- Breeding new varieties of genetically modified organisms
- Pharmaceutical innovation and development
- Control and treatment of AIDS, hepatitis, and other major diseases
- Large aircraft
- High-definition earth observation system
- Manned spaceflight and lunar probe programs
- Classified military projects (x3)

If we take the Major Special Projects as a Chinese technology wish list, we can assume there are two different methods that could be used to achieve these goals. The first involves funding research programmes in universities and companies, educating people over the long term and encouraging a culture of research, development and innovation and an acceptance that achievements in some areas will fall short of expectation.

The second way of viewing the challenge is that much of this technology already exists in the rest of the world, is already proven and is (relatively) easy to obtain. Far easier to steal the work of others, re-engineer it, improve it if practicable and necessary and be seen to be contributing to the progression of the Chinese state; and to do so may also be personally rewarding for members of the Party. Failure to achieve these goals would almost certainly be seen as unacceptable.

At Risk

The companies that generate the target information are not the only ones at risk. We can also assume that the companies that support these areas – lawyers, sub-contractors, outsourced suppliers and any government departments with links to these firms, would also be attacked as part of an effort to find supporting information.

So long as the product is intended for domestic consumption only, in many cases there are minimal problems for the company targeted to have to face. Many firms would be unwilling or unable to sell their products into China anyway – either because of a lack of global distribution networks, or because of export restrictions, in the case of sensitive military technologies, so the sale of an identical, stolen product would not directly harm their business.

For example, a company that makes hi-tech export controlled widgets for the US military is unlikely to be able to sell its product in China to the Chinese military. In any case, the Chinese military would probably prefer to buy a Chinese product. If the widget designs are stolen and a Chinese company makes the exact same widget, protected by a Chinese patent, the end product could be sold to the PLA. While the original manufacturer may rightly be concerned by this, the company would not suffer financially. Until, that is, the product made by the Chinese firm is offered for sale around the world at a much cheaper price than that for which the original product is sold, because the Chinese firm has not needed to fund R&D. At this point, buyers who simply want a widget that works will buy the cheaper one.

The National Outline document goes on to specify 'Frontier Technologies': areas such as biotech, IT, advanced materials and manufacturing technologies, energy and marine technology, lasers and (again) aerospace, all areas in which the West has traditionally excelled and China has lagged behind.

The other key area that could lead to a requirement for cyber attacks is China's intelligence-gathering operation. This area is primarily controlled by the Party rather than the intelligence services themselves. Requirements in this area are likely to incorporate generic tasks to infiltrate and disrupt the activities of the Five Poisons (see above), to gather military secrets from overseas and highlight politically useful information. That could be, for example, intelligence on economic policies of the Eurozone countries regarding China, NATO plans for Afghanistan, international efforts to negotiate with North Korea or reports into human rights abuses.

The intelligence services will use all of their sources – HUMINT, SIGINT and cyber – to address these requirements. As the list is never published we can only guess at what it contains, but one may speculate that if intensive investigations focused on the detection of cyber attacks against the Five Poisons (the GhostNet[14] report was an excellent start), it is likely that the same malware and infrastructure would be revealed to have been deployed.

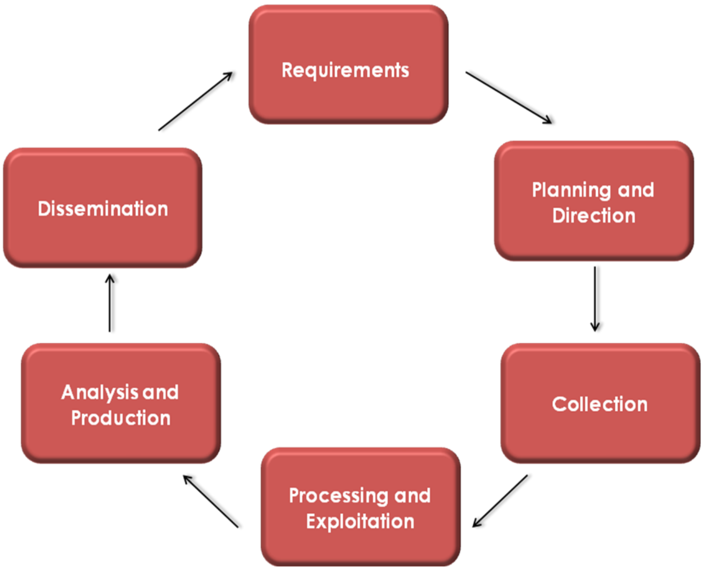
[14] http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

How Does it Happen?

If we consider only the Chinese cyber attacks that have been reported we are only looking at the tip of the iceberg. First, we tend only to see reports of British or American firms being attacked, and we know that only a tiny minority of incidents are reported, because firms are either unaware they have been attacked or are afraid that publicising an incident will damage their brand, their company value or their personal careers. It is also likely that there is a huge number of small to medium sized enterprises around the world that have no idea that their crown jewels have been stolen.

Governments are unlikely to admit having lost data or to accuse China directly, for fear of risking negative political and economic consequences. Individual victims living in China will be unable to complain at the intrusion to their privacy, while those outside China may have little recourse to any organisation which would take their claims seriously.

To map out the process and try to think about the scale of the attacks we must start with a classic diagram of the intelligence cycle.



Setting Requirements

As we have already seen, China has no issue in identifying requirements. These lie across the industrial, social and economic spectrum and represent the results of a mammoth effort to identify weaknesses and areas for further development. Given that the requirements are largely focussed around technical, economic and commercial development rather than social development it is fair to expect that this exercise was not conducted by government alone, but must have been supplemented by private sector (so far as there is one). However, the setting of requirements covers many more areas than just cyber, so it would not be correct to regard this effort as having been conducted simply to support electronic attacks.

Planning and Direction

This is where things get a little bit complicated. Planning and direction activities take place on multiple levels – at a Party level, regional level, local level, within every key government department, inside every company with a stake in fulfilling the requirements; and especially within the military, who evidence suggests are behind the bulk of targeted attacks.

Collection

This area covers the whole process of target identification, malware development, crafting the attacks, designing the social engineering, initiating attacks, controlling implants, escalating privileges on the victim network, uploading further tools to maintain and develop access, finding and exfiltrating data of interest, and cleaning up traces of the attack to hinder investigations.

It also requires infrastructure (owned or stolen) to be constructed to support the attack, IP addresses or domain names updated into the implants, training of operators, language skills, management and some form of quality control process to enable some visibility over how well attacks are progressing.

While much of the attack process can be automated or simplified so it can be delegated to less technically adept operators, the scale of the attack is such that many skilled hackers will be needed in an advisory capacity, to conduct manual elements of the attack, to maintain a development program and, in some cases, to share details of the latest attack vectors and vulnerabilities with those tasked with cyber defence to protect Chinese systems from similar attacks. There will also almost certainly be an administration process that logs attacks and targets, collates information on target systems, feeds data into some form of risk assessment and ensures that all ongoing attacks are focussed on the attainment of a specific requirement. This is no small operation.

Processing and Exploitation

If 1,000 attacks are successful and all result in large amounts of data being stolen from compromised systems, that data needs to be put into a readable format (and decrypted if necessary), made searchable, stored in a database and translated into Chinese – and all these operations have to be carried out in bulk and in real time or something close to it, to allow that information to be used as quickly and effectively as possible. Of course, the actual number of active compromises at any one time is likely to be many magnitudes higher than 1,000!

Analysis and Production

The first problem with analysing bulk amounts of data translated from other languages is that machine translation is often of low quality, particularly for data such as emails written using more colloquial terms. The second issue is that a large proportion of the stolen documents is likely to be of a highly technical nature: If you steal documents from a widget maker then you need at least a basic knowledge of widgets to be able to understand the potential value of a document and how best to exploit it. If there is a lot of widget data you will need a lot of widget specialists or risk the data being out of date by the time it is analysed. And just because someone understands widgets doesn't mean that they understand gizmos, so another team will be required to look at that data – and so on. These analysts will provide feedback to operators, perhaps saying 'get more', or 'this is no good, get something else'. They may also provide search terms for documents. All this analysis will then need to be written up into reports which should try to protect the source of the information.

Dissemination

If the information is to be useful the reporting process has to be fast, in order to get useful information to the right people. Dissemination of intelligence reports to security and intelligence officers should be straightforward as all people in the process will have clearances. But we can assume (although there are no guarantees) that this information is highly classified and dissemination is carefully controlled, which makes disseminating it to government officials a little more difficult, especially if those officials are based outside Beijing, because encrypted links or maybe a network of trusted couriers will be required to transport the reports.

The most difficult task will be delivering reports on commercial or technical development to the right people. The most trusted individuals will be at the top of organisations, probably as a result of their loyalty to the Party, but these are not necessarily the people able to understand, interpret and exploit the information contained within the report. So the report or elements of it must be passed downwards to those who do understand it. This means a significant increase in the number of people who are aware, which represents a significant risk. The Party must also decide to which companies it will pass information – if five companies all produce widgets do you give the information on next generation widgets to one of them, or all of them? We will look at one way the Party addresses this issue below.

Getting the dissemination right should in turn generate more requirements and help to create a more refined requirement to feed back into the process and drive the next data acquisition cycle.

The Scale of the Operation

Most authorities attribute responsibility for cyber attacks and intelligence gathering to the Third Department of the PLA (3PLA) and accept that the Second Department (2PLA) may also have a role to play. Accurate figures for the size of these Departments are not publicly available, but the more success the attackers have, the more funding they are likely to get for further attacks. Other branches of the military may then see the possibility for increased funding and political glory by competing in the same space. One very thorough report by Project 2049[15], a group who analyse the Asian security landscape among other topics, details the Third Department of the PLA and outlines their broader activities and structure. Their role is primarily SIGINT aimed at intercepting radio, telecoms and email communications and reporting the content as intelligence. The report contains a figure (though they make clear this is estimated) of 130,000 people being part of the 3PLA. The 2PLA is concerned with Human Intelligence (HUMINT) as well as SIGINT to support its military intelligence mission.

So trying to work out how many people are involved in this process is only ever going to be based on educated guesswork. If we look simply at the effort in the 3PLA, put aside all other groups for now and take the figure of 130,000 as true, there is a very large pool of available personnel who are able to support cyber operations. However, as we have stated above, the 3PLA has a remit broader than simply cyber and other areas are far more established.

Numbers working in the requirements capture and planning area are probably in the low hundreds. Trying to gauge the size of the collection effort is difficult and requires a large margin of error. But it is fair to assume that several hundred people could do the target development work; around a hundred dedicated specialists could work on malware development (with the Chinese hacking community providing new tools at regular intervals); perhaps one or two thousand low level operators (the 'B' team) supported by another few hundred with more advanced skills (the 'A' team) who look after the most sensitive intrusions; an infrastructure team of a few dozen; and an operational security team of a few dozen more.

Then come the processing and analysis experts: potentially a pool of several thousand specialists able to read and write in a wide variety of languages; hundreds if not thousands of specialists in all of the fields of information being stolen – politics, economics, engineering, IT, science, etc; hundreds of report writers; dozens of people processing data; and dozens more administering the whole process.

If these very rough figures are anywhere close to reality, at least 7,000 people are directly involved in hacking foreign computer networks for the Chinese military and processing the output of those attacks. Potentially many thousands more see the reporting and are aware of the sorts of results generated by these operations.

[15] http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf

Profiting from the Product

So who is most likely to profit from the information being gathered through these attacks? The political, economic and intelligence reporting has a clear audience, but deciding who the commercial intelligence should be passed to presents a more taxing problem. Which companies receive this kind of assistance? The answer may lie in the particular brand of capitalism which China practices.

China is no longer the planned economy it once was and some Chinese companies are now among the largest in the world. But this is not capitalism as we know it and these companies are far from being truly 'private'. All the largest companies in China are State Owned Enterprises (SOEs) in which the state is the largest (or only) shareholder. The state can and does change company board members at will and members of the armed forces are routinely brought into senior management roles. But in addition to simply appointing the heads of companies, the Party also has a final say over the strategic direction of each company, business planning processes and the size of salaries paid to employees. After all, if companies are seen to be profiting unfairly at the expense of the workers that could lead to political unrest.

There are currently 117 companies classed as SOEs and under the control of the State-owned Assets Supervision and Administration Commission (SASAC), the primary shareholder in these companies. To give some idea of the scale of SOEs, they now comprise 80% of the value of China's stock market. Yet in the last 10 years, the number of SOEs has almost halved as SASAC has pushed through mergers of companies with similar strengths to consolidate the overall power of these companies in various sectors and make them more competitive outside China. SASAC works alongside the Communist Party's Organisation Department, which acts as a human resources department and makes certain that those running these businesses care every bit as much (if not more) about pleasing Party bosses as they do about their success in business.

In addition to the Party's input to the strategies pursued by these companies, the state is also instrumental in guiding them to financial success by other means. Most significantly it arranges cheap lines of credit, allowing companies to borrow money for expansion; and provides a ready-made market for the company – the Party has the ability to block competitors from any industry or to introduce policies which make competitors more expensive. The state can also provide considerable human resources if a particular company or industry needs to increase production suddenly: large pools of labour in China work for the state rather than companies and so form a mobile and flexible workforce. But if at the end of the day the products or services a company offers are outdated or of poor quality, that company will fail. The Party has a vested interest in every SOE performing well and becoming a national or global champion in its sector, so it may be willing to extend help through the leveraging of intelligence sources. Note the list of companies and sectors in Appendix A: it is clear that the companies on the list all have interests in areas which will support the Five Year Plan and Indigenous Innovation.

Hypothetical Case Study: Aircraft Construction

One good example of how the Party could use its intelligence collection methods to benefit an SOE is seen in the case of COMAC[16], the Commercial Aircraft Corporation of China. COMAC is currently trying to build a large aircraft to compete with the likes of Boeing and Airbus. In an excellent in-depth paper on Indigenous Innovation[17], the US Chamber of Commerce and strategic consulting firm ACPO Worldwide[18] detail the desire of China to build an aircraft since the crash (and subsequent re-engineering) of a Pakistan Airlines Boeing 707 in 1971. The re-engineered plane named the Yun-10 was a complete failure as China did not at that time possess all the necessary technology required to make it a success.

With a rise in the use of air transport within China, domestic carriers are being forced to buy foreign aircraft at enormous cost, whereas a home-grown aircraft could be sold much more cheaply. The COMAC C919[19] is designed to rival the Boeing 737 and Airbus A320 and planned to be operating by 2015, and to encourage foreign companies to share their technology, China has promised access to the market. Companies including Parker Aerospace, General Electric, Honeywell and Goodrich have all signed up. Whether they benefit from this move in the long term, or are instead encouraged to leave once they have been bled dry of useful information, remains to be seen. But for all the help they are getting, Chinese engineers are not yet able to access the technology developed by Boeing and Airbus, or by large aeroplane engine suppliers such as Rolls Royce.

We know therefore that there is intent to build a domestic airliner and that previously re-engineering has been attempted. Technology transfer is ongoing at the moment, but how (hypothetically) could computer network exploitation attacks help China achieve its goal?

It is hard to imagine that a project of that size would not be given some assistance by the government, given that there is national pride at stake. If intelligence or military resources could be directed against Boeing and Airbus networks there would be some very quick wins. Not only could design documents and technical information be stolen en masse and without the need to actually deal with the company, but there could be some weak links in the supply chains of these companies which would help an attacker to penetrate their networks.

First, smaller suppliers would provide an easy target from where attacks could be launched directly, spoofing emails with Trojans to improve the chance of recipients opening them. Second, both companies have facilities in China, presumably with network connectivity which may provide a direct route into the main network. There are also Chinese citizens working for the two target organisations who could be tasked to download something nefarious or plug in a USB drive to help their country.

[16] http://english.comac.cc/
[17] http://www.uschamber.com/sites/default/files/reports/100728chinareport_0.pdf
[18] http://www.apcoworldwide.com/
[19] http://en.wikipedia.org/wiki/Comac_C919

Finally all large organisations share large amounts of their data with third parties such as law firms and consultants; companies that may not protect their networks as effectively as the target company. These 'data aggregators' can present a major vulnerability in the security of sensitive data.

The end goal of the project is to sell the aircraft worldwide and to undercut the established suppliers. COMAC could achieve this by using lines of credit at favourable rates from the Chinese banks that would help to make deals cheaper for airlines purchasing aircraft. But what really helps these companies undercut foreign rivals is that they have not needed to spend huge amounts of money on R&D to get the plane off the ground in the first place.

If designs for the body of the aircraft could be stolen along with aerodynamic information it would cut development time by years; and by billions of dollars. If stolen engine designs were also used that would cut costs further still. Even if the companies from whom this technology had been stolen were able to see that it had been stolen, they would only be able to take limited action in response; and to do so could put at risk their continued ability to operate or sell in China.

The list of SOEs in "Appendix A" is dominated by transport companies (rail, aerospace and shipping), energy (petrochemical, nuclear, power generation/distribution, hydro), telecoms (mobile, infrastructure), manufacturing, extraction/metals (coal, iron, steel, minerals, aluminium) and trading companies. If a company has been targeted by Chinese state sponsored cyber espionage, we believe that any information stolen probably ends up in one of these SOEs. While China is able to manipulate market conditions in various ways to help SOEs prosper, nothing would contribute more to their growth and success than a supply of inside information about the activities of their competitors and customers.

Conclusion

This situation has not developed overnight. These attacks have been going on for years: many reports detail intrusions going back to 2003 and earlier. It is quite possible that the targets of early attacks were merely foreign governments and dissidents and that the range of targets only broadened with the opening of the Chinese economy and an increased demand for intelligence to support business growth and projects of national importance. The more success the attackers had, the more that demand grew. While China continues to carry out cyber attacks on companies throughout the rest of the world and these attacks continue either unnoticed or unpunished, there is no incentive for China to stop. The more that stolen data is exploited for the benefit of companies and the government, the greater the incentive to continue with these operations.

Governments and large companies do not appear to be making much headway in solving this problem. For large corporations in the West, where there is a tendency to focus more on the short term and on personal achievement rather than the long term advancement of the state, the potential riches which trade with China offers are so large that turning a blind eye to data theft may seem a reasonable price to pay. Governments dare not risk isolation from China for economic and political reasons. Norway has recently been shut out of Chinese relations after awarding the Nobel Peace Prize to a jailed Chinese dissident Liu Xiaobo[20]. Its trade links with China are minimal, so it can afford to do this, but few other countries would feel able to do the same. A combination of this reluctance to act, chronic under-investment in IT and a lack of user education about how to spot the warning signs of a potential attack means companies and organisations are extremely vulnerable.

In order to start rectifying the problem there is a need in the first instance to understand the problem. There needs to be an acceptance that this problem is not going to go away, that this is a business risk not at IT issue. Doing business with China carries extra risk in terms of data security and traditional security products are unable to defend your data against this type of attack. Investigation of compromises needs to be thorough and conducted by people familiar with this problem and not simply the technical aspects of it. Above all sensitive data must be segregated – it is not possible to defend everything.

The reason targeted attacks pose such a dangerous threat is that these are not viruses which simply spread and act according to a set of defined rules in the software. There are human beings directing these attacks in a much more active way. They have been given specific duties and will not stop what they are doing until someone tells them to do so.

If your data is of interest today, it will still be of interest tomorrow. If you have been attacked once and somehow managed to stop it, you have only stopped one instance of the attack, not the attack as a whole. The malware used simply provides a foothold in the network, an initial point of access through which other tools can be uploaded to allow attackers access over the longer term, to navigate through the network until they find the data of interest to them. If one technique doesn't work, they will adapt their methods and raise their game until they have success.

It may be that one day western governments will decide that 'if you can't beat them, join them' and develop similar capabilities to be used against foreign governments and

[20] http://www.bbc.co.uk/news/world-asia-pacific-11505164

companies. We can only speculate as to how China might react to the large-scale targeting of its own companies and institutions. As for now, we have limited evidence of large companies failing as a direct result of the attacks, though there seems to be consensus that Chinese intrusions at least contributed to the downfall of one time telecoms giant Nortel[21]. We do not yet know how many others may follow.

[21] http://www.cbc.ca/news/world/story/2012/02/15/nortel-hacking-shields-as-it-happens.html

About Context

Context Information Security is an independent security consultancy specialising in both technical security and information assurance services.

The company was founded in 1998. Its client base has grown steadily over the years, thanks in large part to personal recommendations from existing clients who value us as business partners. We believe our success is based on the value our clients place on our product-agnostic, holistic approach; the way we work closely with them to develop a tailored service; and to the independence, integrity and technical skills of our consultants.

Context are ideally placed to work with clients worldwide with offices in the UK, Australia and Germany.

The company's client base now includes some of the most prestigious blue chip companies in the world, as well as government organisations.

The best security experts need to bring a broad portfolio of skills to the job, so Context has always sought to recruit staff with extensive business experience as well as technical expertise. Our aim is to provide effective and practical solutions, advice and support: when we report back to clients we always communicate our findings and recommendations in plain terms at a business level as well as in the form of an in-depth technical report.

context
INFORMATION SECURITY

Appendix

No.	Company Name	Website
1	China National Nuclear Corporation	http://www.cnnc.com.cn
2	China Nuclear Engineering Group Corporation	http://www.cnecc.com
3	China Aerospace Science and Technology Corporation	http://www.spacechina.com
4	China Aerospace Science and Industry Corporation	http://www.casic.com.cn
5	Aviation Industry Corporation of China	http://www.avic.com.cn
6	China State Shipbuilding Corporation	http://www.cssc.net.cn
7	China Shipbuilding Industry Corporation	http://www.csic.com.cn
8	China North Industries Group Corporation	http://www.norincogroup.com.cn
9	China South Industries Group Corporation	http://www.csgc.com.cn
10	China Electronics Technology Group Corporation	http://www.cetc.com.cn
11	China National Petroleum Corporation	http://www.cnpc.com.cn/cn
12	China Petrochemical Corporation	http://www.sinopecgroup.com

No.	Company Name	Website
13	China National Offshore Oil Corporation	http://www.cnooc.com.cn
14	State Grid Corporation of China	http://www.sgcc.com.cn
15	China Southern Power Grid Co., Ltd.	http://www.csg.cn
16	China Huaneng Group	http://www.chng.com.cn
17	China Datang Corporation	http://www.china-cdt.com
18	China Huadian Corporation	http://www.chd.com.cn
19	China Guodian Corporation	http://www.cgdc.com.cn
20	China Power Investment Corporation	http://www.cpicorp.com.cn
21	China Three Gorges Corporation	http://www.ctgpc.com.cn/
22	Shenhua Group Corporation Limited	http://www.shenhuagroup.com.cn
23	China Telecommunication s Corporation	http://www.chinatelecom.com.cn
24	China United Network Communications Group Co., Ltd.	http://www.chinaunicom.com.cn
25	China Mobile Communications Corporation	http://www.10086.cn
26	China Electronics Corporation	http://www.cec.com.cn
27	China FAW Group Corporation	http://www.faw.com.cn

No.	Company Name	Website
28	Dongfeng Motor Corporation	http://www.dfmc.com.cn
29	China First Heavy Industries	http://www.cfhi.com
30	China National Erzhong Group Co.	http://www.china-erzhong.com
31	Harbin Electric Corporation	http://www.hpec.com
32	Dongfang Electric Corporation	http://www.dongfang.com
33	Anshan Iron and Steel Group Corporation	http://www.ansteelgroup.com
34	Baosteel Group Corporation	http://www.baosteel.com
35	Wuhan Iron and Steel (Group) Corporation	http://www.wisco.com.cn
36	Aluminum Corporation of China	http://www.chalco.com.cn
37	China Ocean Shipping (Group) Company	http://www.cosco.com
38	China Shipping (Group) Company	http://www.cnshipping.com
39	China National Aviation Holding Company	http://www.airchinagroup.com
40	China Eastern Air Holding Company	http://www.ceair.com
41	China Southern Air Holding Company	http://www.csair.cn
42	Sinochem Group	http://www.sinochem.com
43	COFCO Limited	http://www.cofco.com
44	China Minmetals Corporation	http://www.minmetals.com.cn

No.	Company Name	Website
45	China General Technology (Group) Holding, Limited	http://www.genertec.com.cn
46	China State Construction Engineering Corporation	http://www.cscec.com
47	China Grain Reserves Corporation	http://www.sinograin.com.cn
48	State Development & Investment Corp.	http://www.sdic.com.cn
49	China Merchants Group	http://www.cmhk.com
50	China Resources	http://www.crc.com.hk
51	China National Travel Service (HK) Group Corporation [China Travel Service (Holdings) Hong Kong Limited]	http://www.hkcts.com
52	State Nuclear Power Technology Corporation Ltd.	http://www.snptc.com.cn
53	Commercial Aircraft Corporation of China, Ltd.	http://www.comac.cc
54	China Energy Conservation and Environmental Protection Group	http://www.cecic.com.cn
55	China International Engineering Consulting Corporation	http://www.ciecc.com.cn
56	China Huafu Trade & Development Group Corp.	http://www.hfjt.com.cn
57	China Chengtong Holdings Group Ltd.	http://www.cctgroup.com.cn

No.	Company Name	Website
58	China National Coal Group Corp.	http://www.chinacoal.com
59	China Coal Technology & Engineering Group Corp.	http://www.ccteg.cn
60	China National Machinery Industry Corporation	http://www.sinomach.com.cn
61	China Academy of Machinery Science & Technology	http://www.cam.com.cn
62	Sinosteel Corporation	http://www.sinosteel.com
63	China Metallurgical Group Corporation	http://www.mcc.com.cn
64	China Iron & Steel Research Institute Group	http://www.cisri.com.cn
65	China National Chemical Corporation	http://www.chemchina.com
66	China National Chemical Engineering Group Corporation	http://www.cncec.cn
67	Sinolight Corporation	http://www.sinolight.cn
68	China National Arts & Crafts (Group) Corporation	http://www.cnacgc.com
69	China National Salt Industry Corporation	http://www.chinasalt.com.cn
70	Huacheng Investment & Management Co., Ltd.	Unknown
71	China Hengtian Group Co., Ltd.	http://www.chtgc.com

No.	Company Name	Website
72	China National Materials Group Corporation Ltd.	http://www.sinoma.cn
73	China National Building Materials Group Corporation	http://www.cnbm.com.cn
74	China Nonferrous Metal Mining (Group) Co., Ltd.	http://www.cnmc.com.cn
75	General Research Institute for Nonferrous Metals	http://www.grinm.com
76	Beijing General Research Institute of Mining & Metallurgy	http://www.bgrimm.com
77	China International Intellectech Corporation	http://www.ciic.com.cn
78	China Academy of Building Research	http://www.cabr.com.cn
79	China North Locomotive and Rolling Stock Industry (Group) Corporation	http://www.chinacnr.com
80	China South Locomotive & Rolling Stock Corporation Limited	http://www.csrgc.com.cn
81	China Railway Signal & Communication Corporation	http://www.crsc.cn
82	China Railway Group Limited	http://www.crecg.com
83	China Railway Construction Corporation Limited	http://www.crcc.cn

No.	Company Name	Website
84	China Communications Construction Company Limited	http://www.ccgrp.com.cn
85	Potevio Company Limited	http://www.potevio.com
86	China Academy of Telecommunication and Technology	http://www.datanggroup.cn
87	China National Agricultural Development Group Co., Ltd.	http://www.cnadc.com.cn
88	Chinatex Corporation	http://www.chinatex.com
89	Sinotrans & CSC Holdings Co., Ltd.	http://www.sinotrans-csc.com
90	China National Silk Import & Export Corporation	http://www.chinasilk.com
91	China Forestry Group Corporation	http://www.cfgc.cn
92	China National Pharmaceutical Group Corporation	http://www.sinopharm.com
93	CITS Group Corporation	http://www.citsgroup.com.cn
94	China Poly Group Corporation	http://www.citsgroup.com.cn
95	Zhuhai ZhenRong Company	http://www.zhzrgs.com.cn
96	China Architecture Design & Research Group	http://www.cadreg.com.cn
97	China Metallurgical Geology Bureau	http://www.cmgb.com.cn
98	China National Administration of Coal Geology	http://www.ccgc.cn

No.	Company Name	Website
99	Xinxing Cathay International Group Co., Ltd.	http://www.xxcig.com
100	China Travelsky Holding Company	http://www.travelskyholdings.com
101	China National Aviation Fuel Group Corporation	http://www.cnaf.com
102	China Aviation Supplies Holding Company	http://www.casc.com.cn
103	Power Construction Corporation of China	http://www.zhongguodianjian.com
104	China Energy Engineering Group Co., Ltd	http://www.ceec.net.cn
105	China National Gold Group Corporation	http://www.chinagoldgroup.com
106	China National Cotton Reserves Corporation	http://www.cncrc.com.cn
107	China Printing (Group) Corporation	http://www.cpgc.cn
108	China Guangdong Nuclear Power Holding Corporation Ltd.	http://www.cgnpc.com.cn
109	China Hualu Group Co., Ltd.	http://www.hualu.com.cn
110	Alcatel-Lucent Shanghai Bell Co., Ltd.	http://www.alcatel-sbell.com.cn
111	IRICO Group Corporation	http://www.ch.com.cn

No.	Company Name	Website
112	Wuhan Research Institute of Post and Telecommunications	http://www.wri.com.cn
113	OCT Group	http://www.chinaoct.com
114	Nam Kwong (Group) Company Limited	http://www.namkwong.com.mo
115	China XD Group	http://www.xd.com.cn
116	China Railway Materials Commercial Corp.	http://www.crmsc.com.cn
117	China Reform Holdings Corporation Ltd.	http://www.crhc.cn/n12751492/index.html

Context Information Security Ltd

London (HQ)

4th Floor
30 Marsh Wall
London E14 9TP
United Kingdom

Cheltenham

Corinth House
117 Bath Road
Cheltenham GL53 7LS
United Kingdom

Düsseldorf

Adersstr. 28, 1.OG
D-40215 Düsseldorf
Germany

Melbourne

Level 9, 440 Collins St
Melbourne
Victoria 3000
Australia