The China Security Threat

The threat that China poses to intellectual property and IT security is inducing a degree of caution among Western business executives

By Michelle Price

Information Age, March 2008
http://www.information-age.com/magazine/march-2008/features/313726/the-china-security-threat.thtml

Emboldened and supremely ambitious, the ever-formidable Chinese economy undoubtedly presents an exciting emerging prospect in the flattened landscape of globalised commerce. But the proposition is not without significant caveats. Indeed, had China sceptics required any further suggestion that the country's breathtaking pace of advancement might – at least in some respects – be doing more to indirectly harm Western businesses than to favour them, it has, in recent months, been forthcoming.

Perhaps the most compelling evidence yet to surface emerged at the tail end of November 2007, when anti-virus giant and data security specialist McAfee issued its closely read annual Virtual Criminology Report. Drawing on expertise from the Serious and Organised Crime Agency, the FBI and even NATO, the report outlined the growing threat of web-based global corporate espionage, describing a "new cyber cold war" with "China at the forefront".

Two days later – as if on queue – Jonathan Evans, director general of UK intelligence agency MI5, took the unprecedented step of issuing a warning to UK industry, in which he directly accused China of carrying out state-sponsored espionage attacks against vital arteries of the UK economy. Banks, accountancy firms and legal firms, Evans alleged, are all under electronic attack by Chinese state organisations – including the Chinese army – using the Internet to steal confidential information. Engineering giant Rolls-Royce has fallen victim to these attacks, The Times later reported. In response to these and other revelations, SANS, the renowned training institute for information security specialists, has since placed Chinese-related espionage near the top of its list of cyber security menaces for 2008.

None of which is to say, however, that China is unique in this regard. Web-driven espionage – a natural progression from traditional forms of espionage – is by no means a Chinese preserve. More than 120 countries globally are thought to be developing offensive cyber capabilities, with 30 having made significant advancements, says analyst Gartner. Among them, Russia and Israel – as well as the UK and US – are known to be developing their cyber-competence for defence and military purposes.

But China, the majority of experts agree, is among the most precocious, ambitious and, at present, the most active state globally when it comes to probing – if not overtly aggressive – cyber-activity.

The Opening Salvo

The country has made no secret of its desire to become the world's predominant cyber power. This was starkly underlined in September 2007, when The Times – having gained access to a Pentagon report – revealed that two hackers working for the People's Liberation Army (PLA)

had drawn up a so-called ‘blueprint for cyber war’, in which the electronic crippling of key financial, military and communications networks would serve as the opening salvo to an out-and-out physical conflict.

In such plans, the Pentagon alluded, was clear evidence of Beijing’s ambition to achieve electronic dominance over its global rivals by 2050.

Far reaching as it might sound, the plan is not purely aspirational. According to Paul Sop, CTO of Prolexic, a DDoS-mitigation company that blocks web-based attacks on a daily basis, China’s capability is already evident. “It is strongly suspected that China fields a militia numbering in the tens of thousands – a non-military pool of hackers made up of software engineers, IT specialists and the like – that can certainly coordinate attacks from many global locations.” This has been borne out in a series of well-documented cyber attacks that unfolded during 2007, the chief victims of which were US and European government departments. These included none other than the Pentagon, an attack described by officials as one of the most successful cyber assaults on the US Department of Defense, and an attack on a number of German ministries.

In both cases the attacks were designed to steal information, and in both cases the finger of blamed was pointed at Chinese-based operators – potentially directed or sponsored by the Chinese state government. Closer to home, Whitehall has experienced a number of probes, the aim of which has been to crack passwords and assess vulnerabilities. Elsewhere, the National Informatics Centre in India, the premier science and technology organisation under the Department of Information Technology of the Government of India, as well as New Zealand and Australian official departments have all fallen victim, says McAfee’s Virtual Criminology Report, to focused web-based attacks attempting to steal information, the origins of which appear to lie in China.

Scale and Scaleability

Few will be surprised to learn that, in every instance, the Chinese government firmly denies any allegation of involvement. Proving conclusively otherwise, however, is extremely difficult. First, IP addresses are easily spoofed, meaning that the source from which attacks appear to be emanating may prove false. Secondly, the sophistication of criminal distribution networks, in particular the rise of botnets, also obscures the real actors. Take for example malicious email traffic: according to Secure Computing, a global security appliance provider, Chinese machines are responsible for 9% of all malicious email traffic in the Asian region – a figure that Phyllis Schneck, chair of InfraGard, the FBI-run IT security programme, and vice president of research Integration at Secure Computing, regards as “pretty significant”.

However, she continues, this is not the smoking gun. “All we see is IP addresses sending traffic. It’s therefore hard to know how many people of a certain country are involved. It could be a group based in the US leasing a Chinese botnet.” As China’s grand push towards industrialisation drives Internet connections into the hundreds of million, the size and number of such botnets is likely to surge. Already, says Andrew Colarik, an expert on cyber warfare and author of several books on the subject, China ranks number one in the world for botnet activity, with around nine million infected PCs. To this extent, therefore, the information security threat presented by China is defined – at least in the first instance – by scale. “If you apply the principle

of open Internet to a country as big and as smart as China, your immediate issue is going to be the volume of malicious traffic," Schneck argues.

Evidence provided by information security specialists seems to confirm this. According to Kaspersky Lab, for example, up to 40% of global malware on average emanates from China. Finjan, a gateway security specialist that has been closely tracking global malware in recent months, confirms that China accounts for an extremely high proportion of malicious web activity. In the past three months, however, the company has observed a surge. "We've noticed a major increase in malicious code being sent from servers in China," says Yuval Ben-Itzhak, CTO of Finjan. "This correlates with the announcement that came from MI5. We've noticed that there is a lot of malicious code hosted there, targeting the end users and businesses with Trojans that send back information. Chinese government sites are including this malicious code." Like Schneck, however, Ben-Itzhak is reluctant to point the finger at Chinese operatives specifically. But he does add, "We know that it's very difficult to enforce the law over there: there are usually hackers taking advantages of weaknesses in the law."

Malicious Intent

Nevertheless, many security experts believe that scale is not the only way in which China represents a threat. Evidence surrounding the intent, skill and intensity of aggressive attacks witnessed so far suggests that operators in China – whether closely or only loosely affiliated with the government – have been acting with malicious intent. First, the focus of the attacks has largely been to steal information of a sensitive, oftentimes official or classified, nature. This has been demonstrated clearly by its targets – key players in the Western economy and government departments – as well as by the actual data that is known to have already been relayed back to Chinese IP addresses.

Simon Owen, head of EMEA security at consultancy Deloitte, does not believe this behaviour is consistent with traditional online criminal activity, the pursuit of which is immediate financial gain. In such instances, information theft largely relates to bank account details, online banking login details and personal identity details, all of which are harvested to perpetrate financial fraud – either directly or through identity theft. This activity is usually targeted at consumer-facing websites. Rather, says Owen, who was briefed by the Centre for the Protection of National Infrastructure (CPNI) regarding the CIA's December warning, the information stolen in attacks publicly blamed on China has so far been consistent with the country's economic needs and aspirations. "In China, what we're seeing is very different," he argues. "The Chinese need information to advance their economy. The information they lack is intelligence on advanced Western organisations."

Furthermore, the complexity and intelligence of the attacks has advanced so greatly in recent months that it seems unlikely to be the work of independent operators alone. "Three to five years ago, activity was almost quite basic. There was an awful lot of noise but it was fairly easy to repel if you had your wits about you," says Owen. "During the past 12 to 18 months, the nature of the attacks emanating from the Chinese electronic network is much greater [and] advanced, in terms of style and format and the tools they are using." Finjan has seen what Ben-Itzhak describes as near "cutting edge" malware techniques – including zero-day attacks, sophisticated obfuscation techniques and encryption techniques – that are designed to bypass even best-in-

class security systems. But it is also the strategic sophistication of the attacks that is concerning, adds Owen. “The worrying thing is the intelligence of attack as opposed to the advancement of tools.”

At What Price?

If the web is already proving a major threat, providing a channel for agents in China to target, attack and steal precious IP and sensitive data from Western businesses, then operating within China is certainly no safer. According to the Business Software Alliance (BSA), for example, piracy rates in China are lingering around the 82% mark: for every legitimate software licence in the country, there are more than eight others that are illegitimate. This will necessarily have an impact on Western business models. When Kaspersky Lab first entered the Chinese market, for example, the company took the strategic step of giving its software away for free. Rampant piracy, explains Eugene Kaspersky, the company’s CEO, made attempting to sell the software totally unfeasible within the first few months of entry. “The Chinese copy everything they want. So our strategy was for half a year to give it away to let Chinese people know that we exist.”

According to a well-placed source from an intellectual property body, which has also been working closely with government departments in both Hong Kong and China at large, inadequate protection of IP stems again from the weakness of Chinese law enforcement – particularly in the outer reaches of the country. “The central government wishes to protect IP because they are starting to generate it themselves.” However, he continues, “The government isn’t quite in control. So there is risk and there is opportunity. It’s moving quickly, but [currently] you don’t have a choice: you have to accept that you will be ripped off.”

Technology companies in particular are believed to be targets of this activity. This was boldly asserted by the US-China Economic and Security Review Commission in November 2007. In its report, the committee noted the country’s suspiciously impressive gains in technology development, both at an impressive pace and with impressive quality. The conclusion could only be that the gains were being made at the expense of Western commerce. Indeed, so coveted are the secrets of Western high-tech organisations and infrastructure providers that representatives from the Centre for the Protection of National Infrastructure will only travel to China with a blank laptop, reveals Deloitte’s Owen. “Are they paranoid, or is that an informed view?” he asks rhetorically.

In many respects, identifying the perpetrators of this activity is pointless. In all likelihood, the activity unfolds in three tiers, says Prolexic’s Sop: “Military, state-sponsored and rogue – perpetrated by either politicised groups of individuals operating independently or by cyber criminals motivated by financial gain.”

In many instances, there might be a chain of command that reaches from the government itself or rogue elements in the government. Greg Day, an analyst at McAfee who oversaw the research into the Virtual Criminology Report, does not believe that the government is the chief architect of malicious code, for example. Rather, he suggests, “they are contracting it out”. There is a “big gene pool” from which to choose, he adds.

Either way, it says something fundamental about the present state of the Chinese socio-economic, cultural and legal ecosystem that IP and sensitive data is so sought after, garners such a high price and is so badly protected by the state. Fuelling a juggernaut of an economy clearly requires a significant level of dispersed information appropriation that could, in time, hugely disadvantage Western businesses and the economy at large. The desire to become a supreme economic force also seems to bring with it the desire for military, and therefore cyber, dominance, a status that seems not only to support espionage and data theft, but that will inevitably pose a theoretical threat to Western nations' security, particularly on the mind-boggling scale on which China operates in general. In information security – be it for good or bad – scale is necessarily a significant advantage.

Nonetheless, many commentators believe that a transition in China is already under way. Kaspersky Lab, for example, is now successfully selling its software, having established its brand among a highly discerning, quality-demanding consumer base. As such, the emergence of China might ultimately prove a force for global good, driving up standards, improving quality and fuelling innovation. But the critical question remains: at what price for the West?