PRC Telecoms, Media & Technology Law Newsletter
22 June 2009

MIIT PROMULGATES TWO REGULATIONS FOR REPORTING AND HANDLING CYBERCRIME

Background

1. The first regulations on Internet security in China were promulgated by the State Council in 1994 – the *Regulations for Preserving the Safety of Computer Information Systems* (**1994 Regulations**). These regulations introduced penalties for those who damaged Internet communications or computer systems, or who spread "improper" information that was deemed harmful by the government. The 1994 Regulations assigned the duty of compiling reports on cybercrime and carrying out criminal investigations to the Ministry of Public Security (**MPS**).

2. In 1998, the State Council issued the *Regulations for the Responsibilities, Internal Institutions and Staffing of the Ministry of Information Industry* (**1998 Regulations**). The 1998 Regulations authorized the Ministry of Industry and Information Technology (**MIIT**, then the Ministry of Information Industry) to take action to preserve Internet safety and security. However, they did not require that cybercrime be reported to the MIIT.

   In fact, neither the 1994 Regulations nor the 1998 Regulations assigned the responsibility for reporting cybercrimes or cyber security threats (*i.e.,* information relating to trojan or botnet attacks, serious network failure, or other similar incidents) to any particular governmental agency – including the MIIT. The MIIT and the MPS therefore took on this work themselves on an *ad hoc* basis. The MPS has managed cybercrime, while the MIIT has analyzed and handled Internet security information from a technical perspective.

3. After over two decades, the MIIT has now issued its own regulations on Internet security, which took effect on 1 June 2009. The *Monitoring and Handling System for Trojans and Botnets* and the *Implementing Measures for the Reporting of Cybercrime* (**2009 Regulations**) allocate responsibility for reporting cybercrime and cyber security threats to various designated entities, and reflect the MIIT's desire to be even more proactive in the fight against cybercrime. They thus represent a step toward tighter cyber security policies and affect a wide range of Internet-related entities. It is important to note, however, that as they contain no penalty provisions, the 2009 Regulations lack an enforcement mechanism.

Key Provisions

1. Authorities and Reporting Entities

Pursuant to the 2009 Regulations, the Communications Protection Bureau of the MIIT and its provincial branches are in charge of the supervision and administration of Internet security. The National Computer Network Emergency Response Technical Team / Coordination Centre of China (**CNCERT**) is also authorised to collect, analyze and publish statistics relating to Internet safety information.

Basic telecommunications operators (*i.e.,* telephone service providers), domain name registrars and service entities, the Internet Association of China, and the provincial branches of the MIIT are all responsible under the 2009 Regulations for reporting any Internet safety information of which they become aware to the Communications Protection Bureau and/or CNCERT. Similarly, the CNCERT is responsible for reporting any such information of which it becomes aware (either directly or from third party reports) to the Bureau.

2. Rapid Response System

In an attempt to limit potential damage, the 2009 Regulations set forth time limits for reporting Internet security breaches. Specifically, within two hours of discovering them, the entities listed above must report trojans, botnets and any other serious cyber security breaches and threats to the MIIT or CNCERT, identifying them as either extremely serious, serious, or relatively serious in nature. To accomplish this, the reporting entities and authorities are directed to separately establish and maintain monitoring teams to provide around-the-clock service.

Effects on Market Players

1. Compulsory Requirements for Contract Provisions

The 2009 Regulations expressly require basic telecommunications operators, Internet access providers, IDCs, Internet domain name registrars, and service entities to notify all their users that they, too, are individually responsible for helping to prevent and eliminate cyber security threats. The purpose of this provision is to place the responsibility for cyber security in the hands of the entire Internet community, and thereby further enhance public awareness of trojan and botnet threats. It is also to ensure that cyber security incidents are dealt with swiftly and appropriately, and that hosts or Internet service providers can obligate users to eliminate any trojans or botnets connected to their IP addresses and domain names.

2. "Collateral Damage"

The 2009 Regulations present two significant commercial risks for websites and

software companies: firstly, under the security system introduced by the 1998 Regulations and 2009 Regulations, IP addresses or domain names that have fallen victim to trojan or botnet attacks may be blocked by the MIIT to prevent the spread of malicious programs. As a result, although the 2009 Regulations promote the reporting of cybercrime and ensure a safer Internet environment, some website owners and software producers may incur serious financial losses. Companies and individuals who may be potential targets for an Internet security breach would thus do well to take pre-emptive measures to protect themselves from attack.

The second risk arises from the fact that incidents are analyzed so rapidly that the related findings are susceptible to inaccurate and premature threat assessments. While the 2009 Regulations do not stipulate a precise timeframe its analysis, they do suggest that the MIIT should respond to threats quickly. The MIIT therefore sometimes rushes to analyze and publish information on network failures and similar incidents. This places Internet-related companies at risk for unfounded public scrutiny and bias. For example, when a DNS failure resulted in millions of computers losing access to the Internet on 19 May 2009, the MIIT published a notice stating that the incident was caused by defects in a popular software brand. This culminated in the company issuing a public apology and a free software update. Although it was later discovered that hackers were the source of the problem, the damage to the software company's reputation had already been done.

As the 2009 Regulations increase the operational risks of certain market players, these parties should strive to eliminate the possibility of a trojan or botnet breakout altogether, in order to avoid collateral damage.

3. Possible Software Recommendations by the MIIT

Under the 1998 Regulations, the MIIT is responsible for ensuring Internet safety, and may promote specific software and technological developments for such purpose. The MIIT can even use this authority to require that anti-virus and firewall software which is known to be reliable and effective is provided free of charge with computer purchases. Indeed, it recently ordered that filtering software be included in all new computer purchases after July 1st. Just as the MIIT's filtering software requirement is intended to protect minors from pornography and unhealthy information, standardized anti-virus software could help prevent widespread trojan and botnet attacks.

Analysis

1. Changing Governmental Functions

Since the issuance of the 1998 Regulations, the MIIT and MPS have voluntarily assumed a role in combating cybercrime which is beyond their respective remits from the State Council. However, the MIIT's ability to assess cyber security threats and breaches was hindered by an insufficient reporting system. The

2009 Regulations reflect the MIIT's intention to improve the cybercrime reporting system as a whole, and reflect the MIIT's dedication to combating Internet security threats.

2. Collateral Damage and Pre-emptive Measures

The 1998 Regulations and 2009 Regulations permit the MIIT to shut down websites and cut off IP addresses in order to prevent the spread of trojans, botnets and other threats. They also represent an initial effort at formulating a rapid and organized system for disseminating information to the public on cybercrime statistics, current threats, and prevention methods.

While these initiatives are both laudable, they expose website operators, software companies and other Internet players to commercial risks. By cutting off access to IP addresses and websites, and prematurely – and erroneously – drawing conclusions on the cause or extent of Internet security threats, the MIIT can cause severe reputational and monetary losses to these entities. Industry players would therefore be well advised to adopt their own pre-emptive measures against cybercrime. The MIIT should also carefully assess how to analyse and publicise the information it receives under the 2009 Regulations' reporting system.

3. Future Possible Rules Addressing Penalties

Better administration of cyber security in China is a welcome sight. However, the 2009 Regulations do not stipulate any consequences for those who fail to report Internet safety information within the proposed timeframes. This renders their enforcement difficult and, as the MIIT itself has admitted, effectively reduces the 2009 Regulations to mere guidelines. We therefore anticipate that the MIIT will stipulate penalties in the near future in order to strengthen its efforts to fight cybercrime. Entities subject to reporting obligations under the 2009 Regulations would therefore be well-advised to begin performing those obligations now, in order to become accustomed to them before penalties are introduced. Working through any implementation issues will ensure that things go smoothly once a penalty system is enacted.

Conclusion

Regardless of whether or not the MIIT prescribes a penalty system, the economic consequences of trojan and botnet vulnerability remain. Many trojan and botnet creators generate income by attacking Internet domains and holding them hostage until certain payments are made. Vulnerable systems containing financial information, trade secrets and other sensitive information obviously make easy targets for hackers who can gain access to anything from company strategies to client account details. These risks alone – of compromising financial security and of losing information – should be sufficient to convince market players to take the necessary precautions to protect themselves.

* * *

This article was written by partner Philip Qu (pqu@TransAsiaLawyers.com), together with associates Falcon Yang and Amanda McCreight.

Beijing
Suite 2218 China World Tower 1
1 Jianguomenwai Avenue
Beijing 100004, China
Tel: (86 10) 6505-8188
Fax: (86 10) 6505-8189 / 98

Shanghai
Unit 1101 Platinum
233 Tai Cang Road
Shanghai 200020, China
Tel: (86 21) 6141-0998
Fax: (86 21) 6141-0995 / 6

http://www.TransAsiaLawyers.com

Uploaded on 22.06.2009