S. RAJARATNAM SCHOOL
OF INTERNATIONAL STUDIES
A Graduate School of Nanyang Technological University

RSIS COMMENTARIES

No. 141/2013 dated 29 July 2013

Indonesia:
New Haven for Cybercriminals?

By Senol Yilmaz

Synopsis

Indonesia has been identified as a major source of malicious Internet traffic. A close examination, however, reveals that such traffic may not originate in Indonesia. More likely, Indonesian networks are exploited by outside e-criminals.

Commentary

MALICIOUS INTERNET traffic from Indonesia has increased from 0.7 percent in the last quarter of 2012 to 21 percent in the first quarter of 2013, according to a recent report by private firm Akamai Technologies. This 30-fold increase puts Indonesia at second place after China.

However the rise in malicious traffic does not necessarily mean that Indonesia has become a haven for hackers and e-criminals within a few months. In the report, Indonesia is merely identified as the immediate origin, not the ultimate source, of this malicious traffic.

Indonesian networks being used?

Therefore, it is probable that hackers and criminals from other countries routed their illicit cyber traffic through Indonesian networks to hide their identity and make it more difficult for law enforcement to prosecute them across borders.

At the same time, some countries in the wider region have seen quite a dramatic drop in their malicious traffic. Therefore, the conclusion that Indonesian infrastructure might be misused by other countries' hackers and cybercriminals seems more probable than a sudden increase in the number of homegrown hackers.

The authors of the report assume that the malicious traffic came from so-called botnets, or networks of infected computers. Usually, private users contaminate their computers with malware, or malicious software, by downloading e-mails or files, or by visiting websites that were deliberately infected by criminals. Such contaminated computers, also called "zombies", then allow the criminal, or "botmaster", to command the computers remotely through the malware.

Often, infected computers are exploited for criminal activities without the knowledge of the legitimate private user. For example, the computers in the botnet are misused to spread viruses to other computers or send spam

e-mails. Furthermore, botnets can be used to carry out distributed denial-of-service attacks – the kind of attacks that paralysed Estonia in 2007, when websites of the government, media and banks were flooded with bogus requests for data over a period of three weeks. The networks were overwhelmed by the sheer number of requests and incapacitated to respond to genuine requests. The cyberattacks paralysing the Estonian Internet came from botnets located in several dozen countries.

Challenge to international and national security

The Indonesian government needs to take action for two reasons: international obligation and national security.

Firstly, Indonesia, as any other state, has a duty to prevent both hacking and more severe forms of cyberattacks on its neighbours and states beyond the region. Attacks on other states from botnets located in Indonesia could bring the Southeast Asian country into disrepute internationally – especially when it is government computers that are infected and carry out attacks, albeit unintentionally.

An expert group known as the Tallinn Group, convened by the NATO Cooperative Cyber Defence Centre of Excellence, applied international laws to cyber warfare. Their recently published Tallinn Manual states that under the laws of war, no state shall allow the cyberinfrastructure located in its territory, be it governmental or not, to be used to adversely affect other states.

The experts could not agree on whether this rule applies to malicious traffic merely routed through the cyberinfrastructure of a state's territory. Furthermore, the Tallinn Manual does not constitute international law but represents expert opinion. However, in the absence of treaties, it may be an indication of future law. Notwithstanding, states and private companies who suffered from attacks in the past, are said to have conducted counter-attacks invisible to the international public's eye and beyond legal scrutiny.

For Indonesia, this means that its networks could be disrupted in retaliation for cyberattacks that were neither conducted by the Indonesian government nor its citizens. Therefore, Jakarta should not depend on an ambiguous legal situation, but should take swift action to fight botnets to prevent potential international tensions.

Secondly, and maybe more importantly for Indonesia and Indonesians themselves, botnets can not only be used to attack outside networks, but malicious traffic can also be inbound. In other words, Indonesia could find itself in a situation where its cyberinfrastructure could be attacked and paralysed from within the country. According to a report by the U.S. Congressional Research Service, criminals who command botnets rent their malicious services to anyone who is willing to pay the price of US$200 to US$300 dollars per hour. Non-state actors could rent these botnets to launch cyberattacks against Indonesia's own networks as well as other countries.

Need for action

One approach that has proved useful is to work with Internet Service Providers (ISPs). ISPs play a key role in the fight against botnets since they are in a position to scan their networks and detect infections and abnormal traffic that indicates spamming or denial-of-service-attacks. Co-operation between the public and private sector has proven effective in the German Anti-Botnet project and the Australian Internet Security Initiative. In both countries, once botnet activities are detected, ISPs contact their customers and inform them that their computers are being misused for malicious cyber-activity, and help them clean their infected computers.

Given the increase in malicious Internet traffic from Indonesia, the government should reach out to ISPs to establish a similar project. An important precondition is a sound legal framework that protects the privacy rights of customers while carrying out a programme to fight botnets.

Furthermore, an awareness campaign should be conducted to educate the public of the dangers of computer infections and the remedies available. In the face of these cyberthreats to international and national security, the Indonesian government should take swift preventive action.

Senol Yilmaz is an Associate Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.