CYBERTHREATS - MYTHS OR REALITY?

by
Zahri Yunos and Ahmad Nasir Mohd Zin
National ICT Security and Emergency Response Centre (NISER)

(This article was published in The Star InTech on 9 October 2003)

INTRODUCTION

The dominance and extensive growth of Information and Communication Technology (ICT) makes cyberattacks an increasingly attractive and effective weapon to use against countries. It is attractive to many because it is cheap in relation to the cost of developing, maintaining and using advanced military capabilities. It may cost a little to suborn an insider, create false information, manipulate information or launch malicious logic-based weapons against an information system connected to the globally shared telecommunications infrastructure.

CASES OF CYBERTHREATS

Some people believe that cyberthreats are just a concept others argue that cyberattacks are serious enough to be considered a threat to national security. Some even go to the extent of believing that an Electronic Pearl Harbour is in the making. Even though the public may not know how serious the aftermath may be, the stories of successful cyberattacks should raise some alarms.

Many cases were reported outside Malaysia as a result of cracker activities. For example in 1996, a computer hacker who used the on-line name of “u4ea” had reportedly gained access to the root directories and destroyed the file structures of machines at George Mason University, the University of Arkansas, at a site in the Netherlands, and possibly some U.S. government sites. It is estimated that “u4ea” may have covertly entered more than 100 separate systems.

In another example, 13 root servers that make-up the Internet’s Domain Name Systems were attacked on October 2002. Experts believe that the attacks were coordinated attempts with an objective to totally cripple the Internet (**www.newsfactor.com/perl/story/19756.html**). The source of the attacks could be organised by terrorists or an act of certain governments to test cyberweapons, just like the need to test the nuclear bomb in the middle of the ocean.

The recent major power outage that paralysed the north-east of the United States and Canada on Aug 14, 2003 has raised the question of whether it was the result of a cyberattack. Many have worried about the security of energy control systems in the United States, such as Supervisory Control and Data Acquisition (SCADA) systems that are increasingly being placed online and being opened up to remote access that could contribute to cyberattack (**www.usatoday.com/tech/news/2003-08-18-cyber_x.htm**).

The FBI and the US Homeland Security Department have both said that the outages appeared to be a natural occurrence and not the result of terrorism (**www.post-gazette.com/pg/03227/211976.stm**). However, Al-Qaeda's Abu Fahes Al Masri Brigades has claimed responsibility for the power outage, according to a statement that was reported by Dar Al Hayat, an Arabic newspaper (**http://english.daralhayat.com/arab_news/08-2003/Article-20030818-14bdd659-c0a8-01ed-0079-6e1c903b7552/story.html**).

LOCAL CASE STUDIES INSIDE

Code Red

During the June to November 2001 period, the world community experienced the biggest infrastructural attack in the history of the Internet. Malaysia, unfortunately, was caught in the disaster as well. The Code Red worm initiated a Denial-of-Service (DoS) attack and finally suspends all Internet activities. The variant of Code Red is Code Red II which installs a backdoor into systems it infects. This will allow anyone to remotely run programs or commands on the infected machines that could allow further compromise of the system. Malaysia Computer Emergency Response Team (MyCERT) statistic show that these worms infected 40,652 computers in August 2001, 27705 in September 2001 and 195 in October 2001.

Nimda

Nimda is the first worm to modify existing web document and certain executable files found on the system it infects. Nimda attacks computers that had been compromised by the Code Red worm. MyCERT statistic shows that the Nimda worm infected 9,713 computers in September 2001, 7,654 in October 2001 and 462 in November 2001. The cost of repair is estimated at RM22 million. Note that this does not include the cost of lost business opportunities.

Blaster

Blaster alias "Lovsan" and "Posa") is one of the latest worms that has been infecting computers worldwide. It was discovered on August 11. Blaster exploits the vulnerability in Windows NY, 2000 and XP. As many as 1.4 millions computers may be affected, according to CERT Coordination Centre at Carnegie Mellon University, United States.

According to MyCERT, there were about 500 computers infected with this worm in Malaysia.

Nachi

The new Nachi worm (alias 'Welchia' and 'Blaster.D') is spreading across the Internet on August 19. While Nachi clean up machines that are infected with MSBlast, it creates new network problems by scanning for other vulnerable machines, which consequently causes increased network traffic. This new worm is reported to have caused network problems for many organisations in the country. The estimated cost to eradicate this worm is about RM31mil, not including opportunity cost and productivity cost.

LESSON LEARNED

We cannot continue to solve individual attacks on a case-by-case basis, and not address the larger problem. A better approach is to have an effective coordination amongst the related agencies.

In order to effectively address cyberthreats, collaboration and communication should be both cross sectoral and horizontal to all relevant parties. We all face a common threat with respect to cyberterrorism and need to work together in order to protect our most critical assets. Quick response is a big challenge.

The damage can be stopped quickly if the information flow is fast. This could be achieved if there is a formal relation between stakeholders in invoking their commitment and coordination. Most organisations were slow to respond or deficient in their ability to respond to cyberattacks due to the fact that they did not have the right information on hand.

A common understanding of the threat level could be achieved by sharing information via the provision of vulnerability catalogues, threat alerts and analysis, executive communications, trend briefings, impact analysis etc. The level of threats needs to be defined carefully for the people to have a common understanding. If not, different perceptions and interpretation will occur.

CONCLUSION

The same infrastructure that we utilise to transmit information also creates unprecedented opportunities for criminals, terrorists and hostile foreign countries, who might conduct industrial espionage, cause a vital infrastructure to cease operation, or engage in Information Warfare. The lingering question should not be “will I get hit?” but rather “when will I get hit?”.

Coordinated cyberattacks will definitely come into play sooner in the future. Let us all be forewarned and prepared for all eventualities.