COMPUTER VIRUS: FUTURE CYBER WEAPONS

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

Introduction

The computer virus is generically defined as malicious mobile codes, which include viruses, Trojan horses, worms, script attacks and rogue Internet code. Roger A. Grimes (2001) defined the malicious mobile code as any software program designed to move from computer to computer and network to network, in order to intentionally modify computer systems without the consent of the owner or operator.[1]

A cyber weapon can be defined as a computer programme that is developed or utilised for the destruction of confidentiality, integrity and availability of computer data and systems. Cyber weapons can be divided into three categories – defensive, offensive and dual use. In this article, we shall concentrate on the computer virus, which can be considered as an offensive cyber weapon.

Information Infrastructure as Target

Military strategists argue that a physical attack or bombing against critical infrastructure would disrupt and cripple an enemies' capacity to wage war.[2] During World War II, the Allied Forces applied this theory by destroying critical infrastructure such as electrical power, transportation and manufacturing facilities. The same theory is applied today where a computer virus is used as a weapon to paralyse or cripple the network infrastructure and its equipment.

The recent spate of worms' attack that involves Blaster and Nachi propagation in August 2003 has led some people to speculate that these worms are cyber weapons released to undermine the security of nation states. The recent power outage that hit the North East United States and Canada on Aug 14, 2003 has led some people to make the same speculation. Another incident occurred in January 2003 involving the penetration of the Slammer worm into a private computer network at Ohio's Davis-

Besse nuclear power plant which disabled a safety monitoring system for nearly five hours.[3]

The biggest Internet infrastructural attacks in the world occurred in 2001 and were created by the Code Red and Nimda worms. Malaysia was caught in the disaster as well. According to the Malaysian Computer Emergency Response Team (MyCERT), about 75,533 and 17,829 computers were hit by Code Red and Nimda worms, respectively. Looking at the incidents above, there is high potential that computer viruses will be utilised as a more resilient cyber weapon.

Cramer and Pratt (1996) [4] outlined the characteristics of a computer virus as the following:

a) Size – The size of the program code required for computer viruses is small. This has enhanced the ability of these programs to attach themselves to other applications and escape detection for long periods of time.
b) Versatility – This is the ability to generically attack a wide variety of applications. Most of them do not even require information about the programme they are infecting.
c) Propagation – Once a computer virus has affected a program, the running of the affected program will enable the virus to spread to other programs and files accessible to the computer system.
d) Effectiveness – The many incidents of reported virus attacks have shown that they have far-reaching and catastrophic effects on their victims, which include total loss of data, programs and even operating systems.
e) Functionality – Virus programmes have shown a wide variety of functions.
f) Persistence – After detection, the recovery of data, programmes and even system operation has been difficult and time consuming.

Weapon of Precision Disruption

The characteristics of a computer virus might make it a preferred weapon of precision disruption. The computer virus is called a weapon of precision disruption because of its ability to damage a set of selected targets at a chosen time. E. Anders Eriksson (1999) has given a detailed explanation on this concept.[5] It can also sustain a

prolonged low-impact attack without leaving any trace, but in the long run will result in critical damage to the target. An adversary can mount an attack on a precise target in a controlled manner, without any collateral damage. This is very different from the concept of weapons of mass destruction that incur large scale damage without restrain such as the outcome from nuclear, chemical or biological weapons.

Countries that are incapable of or are prohibited from arming themselves with expensive conventional or nuclear weapons are more likely to use computer viruses as their cyber weapon. Viruses are easy and inexpensive to produce but the impact can be catastrophic. Furthermore, the originator is quite difficult to trace. Developed countries are likely to use cyber weapons as an alternative to conventional weapon or as part of their military arsenal. Computer viruses may be used to complement the usage of conventional weapons.

This is the dilemma faced by advanced countries after the end of the Cold War. The dominance and extensive growth of ICT, makes cyber attacks an increasingly attractive and effective weapon to use against nation states. They realise that other nations that have fallen far behind in terms of military superiority may not be feasible to physical confrontations of weapons and soldiers. They knew that other nations have begun to look for other methods of war-fighting and defence strategies. This led to the development of cyberwarfare strategy, which is also known as asymmetrical warfare.

The Probable Scenario of an Attack

The following illustrates how a malicious programme or code can be used as a cyber weapon.

a) A Trojan is installed in a system of a telecommunication company's main exchange. The Trojan is undetected probably because there is no evaluation conducted on the software or hardware purchased.

b) The Trojan can be activated by an agent through an "insider" or the agent himself by getting a job as an IT employee at the telecommunication company concerned. It can also be activated through satellite signal transmission.

c) The Trojan or the agent activates the "Mole", an undetected hostile programme developed by the adversary. This "Mole" is a program built to conduct surveillance and data collection on computer systems. It listens to traffic and transmits information back through the Trojan horse. This is a highly dangerous threat as the Trojan can open a gateway to every computer system hooked to the core network.

d) Moles are launched into each system including the critical national information infrastructure network. It can be a logic bomb or a virus set to destroy data; and to monitor and steal information.

The above scenario illustrates how a malicious code can be used as a cyber weapon to infiltrate a country's critical national information infrastructure for intelligence purposes or to damage the said infrastructure. The probable results of the attacks are:

a) Crippling the electrical distribution grid by shutting down the control systems

b) Disrupting the national telecommunications network services

c) Sabotaging the airport traffic control systems

d) Attacking oil refineries and gas transmission systems by crippling the control systems

e) Destroying or altering bank information on a massive scale, therefore crippling the financial sector

f) Remotely altering medical information

g) Gaining access to the dam control systems, which can cause massive floods

Conclusion

Computer viruses can be used as a cyber weapon to achieve a strategic objective. It can also be used as a cyber weapon to achieve tactical objectives or for combat usage. It has the ability to disrupt computer systems of radar installations, power grid and communications systems to pave the way for a physical attack, or for safe passage of aircrafts or missiles. Cyber attacks may also cost lives as physical attacks do. Cyber attacks to hospital systems and dam control systems can cause lost of lives. It is not a bloodless weapon.

Countries that are increasingly dependent on ICT, especially those that are connected to the Internet are vulnerable to these kinds of attacks. The paradox is that the more wired a nation is, the more vulnerable it is to cyber attacks. In an era where the use of ICT is a necessity, it is regrettably also highly vulnerable and opens new dimensions of threats in the cyber world. While such development in the area of ICT allows for enormous gains, it has created opportunities to those who have devious ambitions to cause us harm. We have to be prepared for the worst, especially to protect our critical national information infrastructure.

---

[1] Grimes, Roger A., Malicious Mobile Code, Virus Protection for Windows, O'Really & Associates, Sebastopol, California, 2001.

[2] Lewis, James A., Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, December 2002

[3] Slammer worm crashed Ohio nuke plant network, Security Focus, August 19, 2003 <http://www.securityfocus.com/news/6767>

[4] Cramer, Myron L., Dr., and Pratt, Stephen R., Computer Viruses in Electronic Warfare <http://www.infowar.com.survey/virus_ew.html>

[5] Eriksson, Anders, E, Information Warfare: Hype or Reality, The Nonproliferation Review, Spring-Summer 1999.