FUTURE CYBER WEAPONS

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 13 November 2003)

The computer virus is generically defined as malicious mobile codes, which includes viruses, Trojan horses, worms, script attacks and rogue Internet code. Roger A. Grimes defined 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 (Roger A. Grimes, Malicious Mobile Code, Virus Protection for Windows).

Cyber weapon can be defined as computer programme that is developed or utilised for the destruction of confidentiality, integrity and availability of computer data and systems. Cyber weapon can be divided into three categories – defensive, offensive and dual use.

In this article, we shall concentrate on computer virus, which can be considered as offensive cyber weapon.

Information Infrastructure

Military strategists argue that physical attack or bombing against critical infrastructure would disrupt and cripple an enemies' capacity to wage war. 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 computer virus is used a weapon to paralyse or cripple the network infrastructure and its equipment.

The 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 has also led to similar speculation. Another incident occurred in January involving the penetration of the Slammer worm into a private computer network at Ohio's Davis-Besse nuclear power plant and disabled a safety monitoring system for nearly five hours.

The biggest Internet infrastructural attacks in the world occurred in 2001 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 computers were hit by Code Red while 17,829 computers were hit by the Nimda worm.

Looking at the incidents above, there is a high potential that computer virus will be utilised as a more resilient cyber weapon.
Dr Myron L Cramer and Stephen L Pratt (1996) (Computer Viruses in Electronic Warfare) outlined the characteristics of virus as such:

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 – while this affected program is running - the virus is able 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 effect on their victims, which includes 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

The characteristics of computer virus might make it a preferred choice as a weapon of precision disruption. Computer virus is called weapon of precision disruption because of its ability to damage a set of a selected target at a chosen time. E. Anders Eriksson (*Information Warfare: Hype or Reality*) has given a detailed explanation on this concept.

The computer virus can 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 to the target.

This is very different from the concept of weapon of mass destruction that resulted in large scale damage without restrain such as the outcome of the nuclear, chemical or biological weapons.

Countries that are incapable of or prohibited from arming themselves with expensive conventional or nuclear weapons are more likely to use computer virus as cyberweapon. 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 weapon as an alternative to conventional weapon or part of their military arsenal. Computer virus may be used to complement the usage of conventional weapons.

This is the dilemma faced by superpowers 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. Countries realised that other nations in the world 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

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

A Trojan is installed in a system for example a telecommunication company main exchange. The Trojan isundetected probably because there is no evaluation conducted on the software or hardware purchased.

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. The Trojan can also be activated through satellite signal transmission.

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 transmit information back through the Trojan horse.

This is a highly dangerous threat as the Trojan can open gateway to every computer system hooked to the core network.

Moles are launches into each system and 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 purpose or to damage the said infrastructure. The probable results of the attacks are:

- Crippling the electrical distribution grid by shutting down the control systems;
- Disrupting the national telecommunications network services;
- Sabotaging the airport traffic control systems;
- Attacking oil refineries and gas transmission systems by crippling the control systems;
- Destroying or altering bank information on a massive scale, therefore crippling the financial sector;
- Remotely altering medical information; and
- Gaining access to the dam control systems, which can cause massive floods

Conclusion

Computer virus can be utilised to damage the critical information infrastructure of a country. It can also be used as a cyber weapon in achieving tactical objectives or combat usage. It can be used to disrupt computer systems of radar installation, power grid and communications systems to pave the way for physical attack, or for safe passage of aircrafts or missiles.

Cyber attacks may also cost lives as physical attacks do. Cyber attack to the hospital systems and dam controls 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 cyberworld.

While such development in the area of ICT allows for enormous gains, it has created opportunities to those who have devious ambitions to cause harm. We have to be prepared for the worst, especially to protect our critical national information infrastructure.