MILITARY APPLICATIONS OF COMPUTER VARIOUS TO ELECTRONIC WARFARE

By

ABUBAKAR S. YARO

Department of Computer Science School of Sciences
Kwara State College of Education, Ilorin

Abstract

Computer viruses are mysterious and draw our attention. On the one hand, viruses show us how vulnerable we are. A properly engineered virus can have an amazing effect on the worldwide internet and on the other hand viruses show us how sophisticated and interconnected human beings have become.

Most military formations use viruses to attack their enemy country. This paper will be a useful guide to military formations for combat readiness. It will also be a guide to large organizations, institutions and individuals to install anti virus tools and scan through the systems from time to time to check virus attack so as to know them. Since people who listen to different ideas on the risk of offences and uses at least consider that they might be wrong, cannot but gain from this paper.

INTRODUCTION

A computer virus is a program that requires a host in order to make copies of itself on computer disk. Computer viruses are small programs that attach themselves to computer applications and wreck havoc on them. They are programs that spread when infected files are transferred from one computer to another. A virus program will associate itself with another program so that when the program is started, the virus is released at the same time. Some viruses actively destroy software or entire computer system and render it unusable. Some can delete files, some open up a door way to let hackers into the network undetected. Some can be used to initiate denial of service, some cause texts or graphics to be displayed where they are not wanted, some slow down a computer's communications and processing capabilities, while some

just sit there and do not do much of anything. They can cause some significant economic damage.

A computer virus is thus a code that attaches itself to other programs in order to alter their behavior often in a harmful way. Viruses do not care where they are got from, either as an e mail attachment, a download or via a shared disk. Once an infected file or application is opened, the malicious code copies itself into files of the system where they are opened and wait to deliver its payload whatever the programmer designed it to do to a computer system. Simply deleting the e mail after opening the attachment will not get rid of the virus, since it has already entered the computer system where it was opened. A virus writer can set the payload to trigger immediately, at a preset future time or date or upon the execut'on of a specified command such as SAVE or OPEN a file. The Michel Angelo virus for example was programmed to release its payload on March 6th of every year, the birthday of the writer.

As intranets and internet have grown in proportion, e mail has evolved from a convenience to a necessity. Virus's vandals know that and they have invented new ways to use e mail to spread viruses especially worms. A worm program replicates itself and spreads through network connections to infect any computer on the network and replicate itself with it, eating up storage space and slowing down the computer. Worm programs have the potential for sabotage, extortion or blackmail. The name worm was coined as an analogue to a tape worm, a parasitic creature that lives in the intestines of infected human beings and other vertebrates. However, they tend to consume large amount of resources for their own dissemination, thus denying services to legitimate users. The usual lines of attack are the users' mailing lists which contain the names and addresses of other reachable computers. After gaining access to a mailing list, the worm sends copies of itself to some other or all listed computers. The infection usually spreads quickly and downs the entire system by consuming time and network bandwidth so that little or no other work and communication can proceed.

When a person clicks on the attachment, the worm is launched, and then spreads itself by mass mailing itself to all the e mail addresses listed on the infected computers.

DEFENCES AND OUTLOOK AGAINST VIRUSES

Defenses against viruses take generally one or three forms:

i. ACTIVITY MONITORS

Activity monitors are programs that are resident on the system. They monitor activity and either raises a warning or take special action in the event of suspicious activity. Thus, attempt to alter the interrupt table in the memory or to rewrite the boot sector will be intercepted by such monitors. This form of defense can be circumvented by viruses which activate earlier in the boot sector sequence than the monitor code. Another form of monitors are the ones that emulate or otherwise trace execution of a suspect application. The monitor will evaluate the actions taken by the code and determine if any of the activities are similar to that a virus would undertake. Appropriate warnings are issued if suspicious activity is identified.

ii. SCANNERS

Scanners have been the most popular and widespread form of virus defenses. A scanner operates by reading data from disk and applying pattern matching operation against a list of known virus pattern. If a match is found for a pattern, a virus instance is announced. Scanners are fast and easy to use but they suffer from many disadvantages. Among them is that the list of patterns must be kept up to date. In the MS WORD, new viruses are appearing by as many as several dozen each day and week. Keeping patterns file up to date in this rapidly damaging environment is very difficult. Another reason is one of false positive report. As more patterns are added to the list, it becomes more likely that one of them will match some otherwise legitimate code. Again, polymorphic viruses cannot be detected by scanners.

To the advantage of scanners, however, is their spread. Scanners can be made

to work quickly. They can also be done portably and across platforms which are easy to distribute and update. Of the new virus discovered each week, few will become widespread. Scanners equipped with algorithms or heuristic checking may also find most polymorphic viruses. Scanner software looks for a virus in one or two ways. If the virus is known, the software will look for the virus signature that is a unique string of bytes that identify the virus like a finger print and will ZAP it from the system.

iii. INTEGRITY CHECKERS

These are programs that generate check codes e.g checksums cyclic redundancy code in C.P.U, secure hashes, message digits or cryptographic checksums for monitoring files. These checksums or codes are recomputed against the saved. If the comparism fails, a check is known ve occurred to the file and it is flagged for further investigation Integrity monitors run continuously and check the integrity of files on regular basis. The shells check codes prior to every execution. Integrity check is an almost certain way to discover alteration to files including data files. As viruses must alter files to implant themselves, integrity checking will find those changes. Integrity checkers may also find changes caused by buggy software problems in hardware and operator errors. If the self check reveal some unexpected change in memory or on disk, the program will terminate or warn the user. This helps to signal the presence of a virus quickly so that further actions may be taken.

MILITARY APPLICATION OF VIRUSES IN ELECTRONIC WARFARE

Events of the last few years demonstrated dramatically that computer viruses are not feasible but can quickly cause catastrophic disruption of computer systems and networks. Systems have significantly increased the vulnerability of these systems to computer virus attack This has created a new form of electronic warfare consisting in the electronic infections of computer virus micro code into a victim electronic system through direct or indirect mechanism (Myron and Patt, 2006).