ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 6, Issue 2, pp: (64-66), Month: April - June 2018, Available at: www.researchpublish.com

MALEVOLENT PROGRAM

[1]Prof.Jincy C Mathew, [2]Sandeep Naik, [3]S K Khaja Moinuddin

Autonomous College Permanently Affiliated to VTU, Approved by AICTE & UGC
Department of Master of Computer Applications, NHCE, Bangalore, India

Abstract: **Malevolent program (viruses) has been around since the mid 1980s. Over 40,000 different viruses have been cataloged so far and the number of viruses is increasing dramatically. The damage they cause is estimated to be several billions of U.S. dollars per year. Most often, the origin of the virus is difficult to trace. Various kinds of anti-virus software have been developed which detect viruses and take corrective actions. The anti-virus software needs to be continually updated to cope with newer types of viruses. The proliferation of the Internet and Web, have enabled viruses to spread quickly on a massive scale, by taking advantage of several security loopholes. The continual challenge is to have quick and effective responses to these virus attacks.**

Keywords: **Viruses, Malevolent, Security.**

I. INTRODUCTION

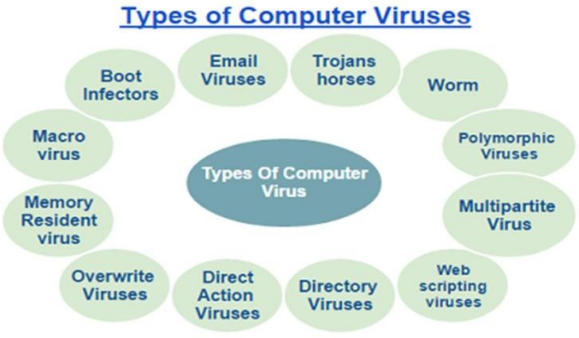
Malevolent program(Computer Virus) is a program that spreads between computers by hiding itself within a seemingly innocent document or application. A worm, on the other hand, is a program that replicates and travels without “infecting” anything else on a system. Many modern specimens of malevolent code, however, use a mixture of tricks to cheat their way onto computer systems, blurring the line between worms and viruses. The terms are now often used interchangeably. The first worms appeared in the 1970s and spread slowly between computers connected to the same network. They simply displayed an annoying message on the screen of each infected machine. The first computer virus, called Elk Cloner, was written in 1982 and infected computers via floppy disks.

Trojans and zombies: But viruses and worms no longer just provide a way for malevolent hackers to gain notoriety. Today’s viral code can contaminate computers at lightning speed, spreading via email, peer-to-peer file sharing networks and even instant messaging programs. The most successful ones cause serious damage, forcing companies around the globe to close down while infected computers are cleaned up.

A string of recent specimens have been designed to snatch passwords or credit card information and install programs that can be used to remotely control infected machines. These programs are known as Trojan horses. There is evidence that virus writers can earn large amounts of money by leasing access to networks of compromised computers – often referred to as “botnets”. These groups of remote-controlled “zombies” have been used to extort money from websites, by threatening to crash them with a denial-of-service (DoS) attack.

This involves overloading a server with bogus page requests, so that real messages cannot get through.

II. TYPES OF MALEVOLENT PROGRAMS



A. Spam:

Spammers have also begun using botnets to forward unsolicited bulk email advertising, or spam, through scores of zombie PCs. This makes it far more difficult for spam hunters to block the messages at source and catch the culprits. Once considered a fairly minor problem, spam is rapidly spiraling out of control, and much more than half of all email messages are now thought to consist of unwanted advertising messages. To combat computer scientists' best efforts to stem the tide of junk email, the spammers have had to become more cunning and sophisticated. More recently, SPIM (spam by instant messenger) and spit (spam by internet telephony) have joined the fray.

B. Phishing:

Spam's more sinister cousin is the phishing email. This is a con trick that arrives as an email and tries to trick a recipient into handing over money or sensitive personal information like their bank account details or a username and password. The simplest phishing tricks try to dupe a target into sending money as part of a get-rich-quick scheme. But phishing tricksters are also getting more devious and recent scams pose as customer service emails and send users to bogus banking or commercial websites where they are invited to "re-enter" their account information.

Some genuine sites have even proven vulnerable to software glitches that can be exploited to capture information from regular users. Phishing is especially threatening because it can be used to steal a person's digital identity.

C. Spyware:

Along with spam and phishing, spyware represents the third of an unhappy trinity of internet pests. These insidious and clandestine programs typically find their way onto a computer system alongside another, often free, software application, although some can also exploit software bugs to get onto a machine. The programs are used to serve up unwanted adverts, change system settings and gather information on a user's online behavior for marketing purposes.

D. Hackers:

The term "computer hacker" was first coined in the 1960s and originally meant someone capable of developing an ingenious solution to a programming problem. But the phrase has since fallen into disrepute, entering the popular vocabulary as a term for a programmer with criminal intent. The earliest "criminal" hackers were in fact relatively harmless, interested in testing the boundaries of their knowledge and their ability to get around security measures. They mainly performed innocuous pranks, for example employing low-tech tricks to get free calls through the US phone networks. There are many tools in the modern hacking kit, including network scanners, packet sniffers, root kits and decompilers. But "social engineering" for example, putting a particularly enticing message in an email header to encourage people to open it and even search engines can also be useful weapons for the hacker.

E. Computer crime:

As the number of computers networks has grown, so have the possibilities for more serious misuse. And, as money increasingly becomes a digital commodity, the world has seen the emergence of serious computer criminals. Criminal gangs have also started to get in on the action, attracted by the huge quantities of money now spent online every day. There is evidence that unscrupulous experts can also earn serious money from crime syndicates by breaking into computer systems, writing viruses and creating phishing scams. And it is not just ordinary desktop computers that are under threat. Governments, banks and critical infrastructure can also be brought to a standstill by an expert armed only with a laptop computer and a net connection.

F. Mobile Phones:

The biggest new target for computer hackers is the mobile device. Virus writers are already experimenting with code designed for smart phones and experts predict more may be on the way, while hackers are also looking at ways to crack handheld devices. While the internet has transformed global communication beyond recognition, the arms race between those intent on harnessing its power for criminal purposes and those tasked with preventing them has only just begun.

III. CONCLUSION

There are lots of viruses in the world and new viruses are coming up every day. There are new anti-virus programs and techniques developed too. It is good to be aware of viruses and other malware and it is cheaper to protect you environment from them rather than being sorry. There might be a virus in your computer if it starts acting differently. There is no reason to panic if the computer virus is found. It is good to be a little suspicious of malware when you surf in the Internet and download files. Some files that look interesting might hide a malware. A computer virus is a program that reproduces itself and its mission is to spread out. Most viruses are harmless and some viruses might cause random damage to data files.

A Trojan horse is not a virus because it doesn't reproduce. The Trojan horses are usually masked so that they look interesting. There are Trojan horses that steal passwords and formats hard disks.

Marco viruses spread from applications which use macros. Macro viruses spreads fast because people share so much data, email documents and use the Internet to get documents. Macros are also very easy to write.

Some people want to experiment how to write viruses and test their programming talent. At the same time they do not understand about the consequences for other people or they simply do not care.

Virus’s mission is to hop from program to other and this can happen via floppy disks, Internet FTP sites, newsgroups and via email attachments. Viruses are mostly written for PC-computers and DOS environments.

Viruses are not any more something that just programmers and computer specialist have to deal with. Today everyday users have to deal with viruses.

REFERENCES

[1] Keihänen T., TKK:n virusopas, TKK Offset 1996, pp 3-11

[2] Lammer V., Computer Viruses, Virus Bulletin '93

[3] Helenius M., Computer viruses in Finland - A questionnaire survey, University of Tampere 1994

[4] Koskinen P., Tietokonevirusten teko ja levitys aiotaan säätää rangaistavaksi, Helsingin Sanomat 12.11.1997

[5] Sudduth A., The What, Why, and How of the 1988 Inernet Worm, 1988

[6] http://www.tml.tkk.fi

[7] VX Heavens, http://vx.netlux.org/

[8] Orr, “The viral Darwinism of W32.Evol: An in-depth analysis of a metamorphic engine,” 2006. http://www.antilife.org/files/Evol.pdf

[9] Orr, “The molecular virology of Lexotan32: Metamorphism illustrated,” 2007. http://www.antilife.org/files/Lexo32.pdf

[10] https://www.Quora.com

[11] https://en.wikipedia.org/wiki