IJARESM
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING, SCIENCE & MANAGEMENT

COMPUTER AND MOBILE VIRUS: A CHALLENGE FOR INFORMATION & COMMUNICATION TECHNOLOGY PROFESSIONALS

Ronak K Panchal[1]
Assistant Professor, Vidyabharti Trust College of BCA, Umrakh, Bardoli, Gujarti, India[1]

Abstract: Nowadays, Information communication technology has become part of our life. Everything is becoming digital day by day. How to origin virus, spread it and to damage it? How virus is work in Computer and Mobile which are mention. In this research we can direction and guidance of types, Symptoms and antivirus software of Virus.
Keywords: virus, computer virus, mobile virus, antivirus.

INTRODUCTION

Nowadays technology has become part of our life. Everything is becoming digital day by day. Information communication technology is used in every field including computer systems. Almost all activities such as documentation centers, knowledge resource centers, and wireless communication are done using computer systems with latest software technology.

While carrying out any activity it is obvious that problems will arise. So, having a brief knowledge and idea about the cause of those problem and possible solutions of such problem is an advantage. All ICT professionals are not well versed with the aspects of computer and mobile viruses. So, there is need to take initiative to aware them about these viruses their functioning, damages caused by them and remedies to deal with them.

1. COMPUTER VIRUS

Computer virus are a type of software program that, like a biological virus reproduces and spreads itself as in case of the biological virus with the computer virus too, many times the damage takes place before the victims are aware of its existence. A program that attempts to spread from computer to computer and either cause damage (by erasing or corrupting data) or annoy users (by printing messages or altering what is displayed on the screen). The full form of **Virus** is *Vital Information Resources under Seize* (Virus).

A virus can affect the normal functioning of the computer in many ways. Whereas some virus may display only a message on the screen, others may slow down your PC or many causes extensive damage to your system. For instance they may change computer files so that program does not correct properly or even stop working. They can also erase files or even format your CD or Hard-disk and crash the system. Computer viruses are also famous with names such as worms, bugs, Trojan horses, malware, spyware etc.

2. MOBILE VIRUS

A **mobile virus** is software that targets *mobile phones* or *wireless-enabled PDAs*. As wireless phone and PDA networks become more numerous and more complex, it has become more difficult to secure them against electronic attacks in the form of viruses or other malicious software (also known as malware).

Viruses can be disguised through sms or an email attachment as an enticing image, audio or video files or even a greeting card through the Bluetooth. This means that unless you are expecting an email attachment or you know the source of one, do not open any from an unknown source.

3. HISTORY OF COMPUTER VIRUS

Traditional computer viruses were seen in 1980. The reason of their emergence was:

1) Spread of personal computers (PC's) in business, homes and college campuses
2) Use of computer bulletin boards. People could dial up a bulletin board with a modem and download programs of all types. This enabled emergence of Trojan horse
3) Creation of floppy disk which enabled emergence of first self replicating program virus

4. HISTORY OF MOBILE VIRUS

The first instance of a mobile virus occurred in June 2004 when it was discovered that a company called Ojam had engineered an anti-piracy Trojan virus in older versions of their mobile phone gameMosquito. This virus sent SMS text messages to the company without the user's knowledge. This virus was removed from more recent versions of the game; however it still exists on older, unlicensed versions. These older versions may still be distributed on file-sharing networks and free software download web sites.

In July 2004, computer hobbyists released a proof-of-concept mobile virus named Cabir. This virus replicates itself on Bluetooth wireless networks.

In March 2005 it was reported that a computer worm called Commwarrior-A has been infecting Symbian series 60 mobile phones. This worm replicates itself through the phone's Multimedia Messaging System (MMS). It sends copies of itself to other phone owners listed in the phone user's address book.

In August 2010, Kaspersky Lab reported the first malicious program named Trojan-SMS.AndroidOS.FakePlayer.a classified as a Trojan-SMS has been detected for smartphones running on Google's Android operating system. It has already infected a number of mobile devices. It sends SMS messages to premium rate numbers without the owner's knowledge or consent which can rake up huge bills. For a security concern, Android users are advised to download from a trusted source.

5. ORIGIN OF COMPUTER VIRUS

A person creates virus by writing code in particular computer language & scripts, test it to make sure it spread & then release it. That person is called computer virus programmer. There are three reasons for creation of virus:

- Interest of the people to feel the thrill of watching blast by making virus
- Psychology of people to create things of destruction for human society

- To make profit, to earn money by making virus

6. ORIGIN OF MOBILE VIRUS

According to research, China currently leads the relay in mobile virus development, followed by Brazil and a notable portion of the current viruses are even created in Turkey, with which the countries of the former USSR can be compared best to right now regarding virus production.

The former USSR(Union of Soviet Socialist Republics) has come up with four copies or mobile viruses, but three of them have been conceptual viruses, meaning the first of their kind.

- The first backdoor program for WinCE, which received the name Brador, was provided by a programmer from the Ukraine, famous by the nick name BrokenSword.
- The second worm ComWar's origin is Russian, too as testified by texts contained in the virus and available information about the author e10d0r.
- The third is the Trojan RedBrowser, whose creator is unknown, but the texts in the Trojan as well as the telephone numbers that send the SMS clearly prove its Russian origin.

7. HOW COMPUTER VIRUS WORKS

A Virus is a small piece of code embedded in a larger legitimate program. When the user runs the legitimate program, the virus loads itself into memory and looks around to see if it can find any other programs on the disk. If it can find one, it modifies the program to add the virus's code into the program. The virus now produce itself so two programs are infected. The next time the user either of those programs they infect other programs or the cycle continues.

E-mail Virus A Virus travels as an attachment with e-mail message and replicate itself, by automatically mailing itself to dozens of people in the victim's e-mail address book.

E-mail virus such as Melissa virus(March,1999) resides in internet newsgroup. Anyone who downloaded the document & opened it would trigger the virus. The virus would then send the document in an email message to first 50 people in the person's address book. Email containing friendly note with person's name. it results in infected 50 machines the virus would then created 50 new messages from the recipient machine.

Spam Spam is the e-mail version of junk mail. It means to send undesired message indiscriminately to multiple mailing lists, individuals, or newsgroups. The word used by geo. A. Hormel & co. in U.S. 1937. A common synonym for spam is unsolicited bulk e-mail(UBE). All the infected messages can be moved to spam an option available in e-mail account to make it free of virus.

Fire Fire is regarded as one of the most hazardous enemy of libraries. Usually we do not give emphasis on what is the condition of electric points, sockets, main electric point, and status of writing in a library. A librarian may not know much about the electricity but it is his duty to assure that everything is in good condition. Fire may occur in two ways:

- Fire caused by Electricity

- Normal fire caused by human mistakes Safety of computer systems containing precious electronic database, library records and software from fire is most important issue. We can do the following to deal with it:
- We should check that electronic sockets, plugs and wiring of library are of best quality and ISI marked.
- The library should have all the fighting equipments available as a preventative measures for unexpected fire accidents
- Staff of the library should be trained to deal with fire accidents

8. HOW MOBILE VIRUSES SPREAD

Previously, mobile viruses differed from computer viruses in using specific ways of propagating - via Bluetooth or MMS. However, the functionality of the .NET programming platform which is integrated into WinCE has enabled virus writers to exploit yet another, more traditional infection vector: email. For example, the Letum worm behaves in exactly the same way as thousands of typical PC email worms: once it gets onto a phone, it sends itself to all the email addresses stored in the infected device's contact list. Furthermore, Letum could be classified as a cross-platform virus, as it is capable of running on computers running .NET.

Cross platform viruses The Cxover virus is the first cross-platform malicious program for mobile phones. When launched, it checks to see which operating system is running, and when launched on a PC, it looks for access to mobile devices via ActiveSync. The virus then copies itself to the mobile device using ActiveSync. Once it is on the mobile device, the virus attempts to perform the procedure in reverse, i.e. to copy itself to the PC. It can also delete user files on the mobile device.

The Mobler worm works a little differently. Once it's launched on a PC (with a Win32 component), it creates a SIS file on the E: drive. The SIS file contains several empty files which are used to overwrite a number of system applications on the phone. The file also contains the worm itself which then copies itself to the phone's memory card and adds a file called autorun.inf. If a user connects a Mobler-infected phone to a computer and tries to access the phone's memory card, the worm will automatically launch and infect the computer. Mobler is a clear example of a cross-platform virus capable of running on totally different operating systems: Windows and Symbian.

New platforms Prior to 2006, the two most frequently attacked mobile platforms were Symbian and WinCE, which are the main smartphone platforms. The appearance of the RedBrowser Trojan in February 2006 was an unpleasant surprise. This was the first time that standard handsets (i.e. not smartphones) were infected. RedBrowser targeted mobiles which use the J2ME platform to run certain applications.

Although until recently it seemed an impossibility, infecting almost every kind of mobile phone is now a reality. The very appearance of Trojans for J2ME is just as worrying as the appearance of the first worm for smartphones in June 2004. It's still difficult to assess all the potential threats. However, it's a fact that the standard handsets still outnumber smartphones and malicious users have now worked out how to infect a standard phone and use it for

criminal purposes. This means that antivirus protection for such devices is becoming a relevant issue.

Also in 2006, the first proof of concept backdoor for BlackBerry devices was detected. However, it was written in Java, and according to Kaspersky Labs, therefore can't really be classified as malicious code for a new platform.

9. SYMPTOMS OF COMPUTER VIRUS

- You see strange massages on the screen eg ***Your PC is stoned*** or ***happy birthday to you***
- Letters look like as they are falling to the bottom of the screen
- Program suddenly takes long to load or execute or they stop working
- The computer system becomes slow
- The size of the program system file keeps changing
- The size of the available free memory reduces
- Hard disk runs out of space
- Strange file appears with strange names on your hard disk
- Unable to access the hard disk or CD
- The computer does not boot
- Program or data files get damaged(corrupted)
- Clicking noise comes from the key board
- Your computer stops responding or lock up often shows-"Not Responding"
- Your computer crashes and restarts every few minutes
- Your restarts on its own and then fails to run normally
- Applications on your computer don't work correctly
- You can't print correctly
- You see distorted menus and dialog boxes

Way through which computer virus spreads:

- While installing, downloading any file object from internet
- While copying, editing anything from an infected CD's pen drives
- While downloading some illegal, private, unauthorized files and objects from internet or any local disk borrowed from friend
- Virus can enter through email if it contains infected files
- Scan CD, pen drive, DVD, after inserting it in computer to check virus

10. SYMPTOMS OF MOBILE VIRUS

- Your phone may go into re-starting frequently.
- Your phone may operate slower than usual.
- Your phone may stop obeying commands or locks up often.
- You may not be able to access some applications in your phone.
- Some applications on your phone may refuse to work properly.
- Unusual error messages may occur often and menus may appear unclear.
- Installed antivirus is likely to be disabled or the program may not start.
- Icons which you did not put may crop up and recently opened attachments may have dual extensions.

- New antivirus cannot be installed and even if it is installed, it will refuse to work until the phone is debugged.
- Battery depletion rate is likely to increase because the virus through its malicious operations will over labor the battery.

11. TYPE OF COMPUTER AND MOBILE VIRUS

- File overwrite virus
- Jokes(JOKES)
- Security Privacy Risk(SPR)
- Unusual runtime packers(PCK)
- Double Extension File(HEUR-DBLEXT)
- Phishing
- Adware
- Backdoors
- Boot viruses
- Hoaxes
- Macro viruses
- Pharming
- Polymorph viruses
- Program viruses
- Root – Kit
- Script viruses and worms
- Spyware
- Trojan horses(Short Trojans)
- Cabir
- Duts
- Skulls
- Commwarrior

File overwrite virus File overwrite viruses infect files by linking themselves to a problem. They keep the original code intact and add themselves to as many files as possible. The simple version of file overwrite do not cause any damage though they still take up hard disk space as they increase the size of the several files and slow the performance.

Jokes(JOKES) Jokes are merely intended to give someone a fright or provide general amusement without causing harm or reproducing. When a joke program is loaded, the computer will usually start at some point to play a tune or display something unusual on the screen. Examples of jokes are the washing machine in the disk drive (DRAIN.COM) or the screen eater (BUGSRES.COM).But bewares! All symptoms of joke programs may also originate from a virus or Trojan. At the very least users will get quite a shock or be thrown into such a panic that they themselves may cause real damage.

Security Privacy Risk (SPR) Software that maybe is able to compromise the security of your system, initiate unwanted program activities, damage your privacy or spy out your user behavior and might therefore is unwanted.

Unusual runtime packers(PCK) Files that have been compressed with an unusual runtime compression tool and that can therefore be classified as possibly suspicious.

Double Extension File(HEUR-DBLEXT) Executable files that hide their real file extension in a suspicious way. This camouflage method is often used by malware.

Phishing Phishing, also known as brand spoofing is a clever form of data theft aimed at customers or potential customers of internet service providers, banks, online banking services, registration authorities.

When submitting your email address on the internet, filling in online forms, accessing news groups or websites, your data can be stolen by “Internet crawling spiders” and then used without your permission to commit fraud or other crimes. Phishers generally send their victims’ actual official letters such as emails that are intended to induce them to reveal confidential information to the culprits in good faith, in particular user names and passwords

or PINs and TANs of online banking accounts. What is clear is that banks and insurance companies never ask for credit card numbers, PINs, TANs or other access details by email, SMS or telephone.

Adware Adware is software that presents banner ads or in pop-up windows through a bar that appears on a computer screen. These advertisements usually cannot connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

Backdoors A backdoor can gain access to a computer by circumventing computer access security mechanisms. A program that is being executed in the background generally enables the attacker almost unlimited rights. User's personal data can be spied with the backdoor's help, but are mainly used to install further computer viruses or worms on the relevant system. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

Boot viruses The boot or master boot sector of hard disks is mainly infected by boot sector viruses. They overwrite important information necessary for the system execution. One of the awkward consequences: the computer system cannot be loaded any more.

Hoaxes For several years, internet and other network users have received alerts about viruses that are supposedly spread via email. These alerts are spread per email with the request that they should be sent to highest possible number of colleagues and to other users, in order to inform everyone against the "danger".

Macro viruses Macro viruses are small programs that are written in the universal language of an application (e.g. WordBasic under WinWord 6.0) and that can normally only spread within documents of this application. Because of this, they are also called document viruses.

Pharming Pharming is a manipulation of the host file of web browsers to divert enquiries to spoofed websites. This is a further development of classic phishing. In the case of a manipulation of the host file, a specific manipulation of a system is carried out with the aid of a Trojan or virus. The result is that the system can now only accesses fake websites, even if the correct web address is entered.

Polymorph viruses Polymorph viruses are the real master of camouflage. They change their own programming codes – and are therefore very hard to detect.

Program viruses A computer virus is a program that is capable to attach itself to other programs after being executed and cause an infection. Viruses multiply themselves unlike logic bombs and Trojans. In contrast to a worm, a virus always requires a program as host, where the virus deposits his virulent code. The program execution of the host itself is not changed as a rule.

Root – Kit A root kit is a collection of software tools that are installed after a computer system has been infiltrated to conceal logins of the infiltrator, hide processes and record data – generally speaking: to make themselves invisible. They attempt to update already installed spy programs and reinstall deleted spyware.

Script viruses and worms Such virus are extremely easy to program and they can spread – if the required technology is on hand within a few hours via email round the globe. Script viruses and worms use one of the script languages, such as JavaScript, VBScript etc., to insert themselves in other, new scripts or to spread them by calling operating system functions. This frequently happens via email through the exchange of files (documents).

A worm is a program that uses computer networks and security holes to replicate itself in hard disk and memory but does not infect the host. Worms can consequently not form part of other program sequences. Worms are often the only possibility to infiltrate any kind of damaging programs on systems with restrictive security measures. It consumes space and resources without attaching itself to other programs.

Spyware Spyware are so-called spy programs that intercept or take partial control of a computer's operation without the user's informed consent. Spyware is designed to exploit infected computers for commercial gain.

Trojan horses(Short Trojans) Trojans are pretty common nowadays. We are talking about programs that pretend to have a particular function, but that show their real image after execution and carry out a different function that, in most cases, is destructive. Trojan horses cannot multiply themselves, which differentiates them from viruses and worms. Most of them have an interesting name (SEX.EXE or STARTME.EXE) with the intention to induce the user to start the Trojan. Immediately after execution they become active and can, for example, format the hard disk. A dropper is a special form of Trojan that 'drops' viruses, i.e. embeds viruses on the computer system.

Lasco: The worm Lasco appeared as the first of these independent families. Apart from usual worm functionalities, it can also infect files, too.

Pbstealer: This harmful program was developed in China and was discovered on a hacked Korean Webpage with the online game "Legend of Mir".

This Trojan overtook Cabir in Bluetooth spreading, but the authors also made this time an important change in the source code: The Trojan selects the address database of the mobile phone and stores it in a text file. This is dispatched via Bluetooth to the next found device at hand. This is where the designation Pbstealer -"Phonebook Stealer"- comes from.

Cabir: Infects mobile phones running on Symbian OS. When a phone is infected, the message 'Caribe' is displayed on the phone's display and is displayed every time the phone is turned on. The worm then attempts to spread to other phones in the area using wireless Bluetooth signals.

Duts: A parasitic file infector virus and is the first known virus for the PocketPC platform. It attempts to infect all EXE files in the current directory (infects files that are bigger than 4096 bytes).

Skulls: A trojan horse piece of code. Once downloaded, the virus, called Skulls, replaces all phone desktop icons with images of a skull. It also will render all phone applications, including SMSes and MMSes useless.

Commwarrior: First worm to use MMS messages in order to spread to other devices. Can spread through Bluetooth as well. It infects devices running under OS Symbian Series 60. The executable worm file, once launched, hunts for accessible Bluetooth devices and sends the infected files under a random name to various devices.

12. SOME WAYS OUT TO DEAL WITH THESE VIRUSES

- Install only registered, standardized, safe and protected antivirus in your computer
- Install a firewall which will protect all viruses to enter your computer/LAN.
- Always keep your antivirus in active mode and do scanning of the computer everyday

13. ANTI VIRUS

These are programs written in programming languages like c++, java and visual basic scripts and other such computer languages to kill and to reduce and to reduce the effect caused by viruses. Anti virus software detects and eliminates known computer viruses before damage occurs.

Viruses are destructive programs that spread from computer to computer over the Internet or a network. Viruses can be attached to other files or disguised as files that look ordinary. Computer can be protected from viruses and other security threats by:

- Installing and using up-to-date antivirus software
- Setting up your e-mail and internet software so that it is more difficult for files containing viruses to make their way onto your computer at all

In addition to using up-to-date antivirus software, it should be a "real – time scanning" antivirus (depending on the brand of software, this feature might have another name). Real time scanning checks files before they are opened.

Some of the best anti-viruses available in the market are listed below:

- AVG Anti-Viruses
- Avast Anti virus
- Avira Anti Viruses
- Symantee anti viruses
- Norton anti viruses
- McAfee virus scan
- PC-illin anti virus
- F-port professional
- IBM anti virus
- Dr. Solomon's Anti virus
- Quick Heal
- Bit Defenders

Firewall A combination of hardware and software that provides a security system, usually to prevent unauthorized access from outside to an internal network or internet is referring as firewall. A firewall prevents direct communication between network and external computers by routing communication through a proxy server outside of the network. The proxy server determines whether it is safe to let a file pass through to the network. A firewall is also called a security - edge gateway.

Mirror site Keeping library records, databases and other important information at different disk / servers / locations or places (sites) for their safety is called as mirror sites. If one mirror site becomes unavailable (due to a disk failure, for example), windows can use the remaining mirror site to gain access to the volume data. Mirror volumes can be created only on dynamic disks. For e.g. Indian railways server having important dynamic database at two to three different locations as mirror sites which is useful incase of damage of databases in fire accidents.

Pop up An option that appears on top of the browser window when a computer user logs on to a web site or selects an option displayed on it. Usually covering a portion of the screen. Some web sites burden the viewer with multiple popup containing advertising. Popup are obtrusive because they block from view material displayed in the browser window, requiring the user to either select an option or close the popup window to see underlying content.

14. BACK UP

Back up is keeping spare copy of file, file system or other resource at different sites for use in the event of failure or loss of the original. It is important to keep the double copies of files at different sites to avoid the damage due to a disk crash or accidentally delete of files

on which one may be taken in CD's, storage device, in hard disc in another folder every day or once in week depending upon the need.

CONCLUSION

While performing every activity we come across many problems but if we have right direction and guidance the solution of such problems but if we have right direction and guidance the solution of such problem can be found easily. Virus becomes the most difficult problem we are facing nowadays. But nowadays solution of every virus is also coming up. But creation of virus and finding solution of virus in the form of antivirus for earning the money and for the marketing of anti viruses has become the trend of the moment. So many anti viruses are available nowadays to deal with viruses.

REFERENCES

[01] R. K. Taxali (2000) Computer viruses and Email. PC Software book is used in BCA syllabus
[02] http://www.wikipedia.com
[03] http://mobilephonevirus.barabasilab.com/research.html
[04] http://www.yourmobileinfo.com/tag/tips-on-mobile-phone-virus-symptoms/
[05] http://en.wikipedia.org/wiki/Mobile_virus
[06] http://mobilephonevirus.barabasilab.com/research.html
[07] http://www.yourmobileinfo.com/tag/tips-on-mobile-phone-virus-symptoms/
[08] http://service-handphones.blogspot.in/2011/08/tips-on-mobile-phone-virus-symptoms.html
[09] http://www.mediabuzz.com.sg/asian-emarketing/september-october-2009/618-the-origin-of-mobile-viruses