RESEARCH ARTICLE OPEN ACCESS

Epidemiological Imitation of Computer Virus

Sudeesh Kumar G and Puja Roy
Seth M. R. Jaipuria School, Padrauna
Ghagra High School, Alipurduar

Date of Submission: 16-04-2020 Date of Acceptance: 01-05-2020

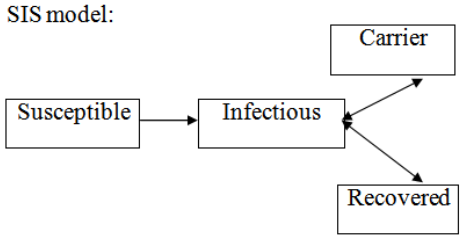
I. INTRODUCTION

Virus-Vital Information Resources under seize, Computer virus is a malicious program that can reproduce itself and can be extend or spread from computers to computers. When the reproduction or replication succeeds the affected areas are said to be the areas infected with the computer virus. Once breaking out a virus can perform destructive operations in a computer such as modifying the data, deleting of data, removing or erasing file or contents, encrypting the files and formatting of the disks.

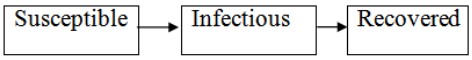
Virus coding programmers use social engineering deceptions and make use of the detailed knowledge of security weakness to initially infect the systems and to spread the viruses. Computer viruses can cause very huge economic damage every year by causing system failure, wasting of the system resources, corrupting and deleting data increase the cost of maintenance or stealing of the personal information. Very huge outbreaks of computer viruses has bought huge economical loses. With the start of new era of IoT (Internet of Things) and cloud computing the threat from viruses has enhanced to a serious level even leading to havoc. The tern virus is also used in a wrong way or measured by extension for referring other types of malwares. Malwares encompasses the computer virus along with many others types or forms of malicious software such as computer worms, Trojan horses, ransom wares, spywares, key loggers, root kits , Boot kits etc. we know that Antivirus program or software is the main means of shield against the virus. With the frequent emergence of the new forms of the existing types of virus as well as new types of virus strands, the fight waged by the humans against the virus is doomed to be endless, very difficult and conniving , indeed the development of the new types of Antivirus programs always delayed behind the emergence of new forms of virus. As the Antivirus technique cannot calculate or predict the evolution trend of the viruses and thus cannot provide universal suggestion for their prevention and control.

Compartmental models in Epidemiology:

SIS model:



SIR model:



The Compartmental models in the Epidemiology should define the speed at which susceptible individuals get infected and the speed at which the infected individuals recover. enthused by the intriguing analogies between the computer virus and their biological equivalents creatively suggest that the technique developed in the epidemic dynamics of the contagious disease should be exploited to study the spread of the computer virus. The SIS model can be used later to find the way how the viruses multiply on the internet.

The researches has been classified into two different directions

(i) The finding that the independent system level arrangement structure of the internet follows a diverse power law distribution, means relative change in one quantity results in proportional relative change in another (Scaling law) has fueled the interest in spreading the behavior of the viruses on the complex network. The past works in this direction are focused on the existence and evaluation of epidemic speed under the SI model. The SIR and SIS model leads to the most interesting findings that the epidemic rate fades away for the free scale network with inestimable amount.

(ii) To understand the wide spreading of the computer viruses has forced the proposal of many types of epidemic models that are fully based on completely connected networks, which means the

network where all computers can equally access the other computers in the network.

This paper is proposed to bring in front a series of epidemical models of the computer virus and a deep and close examination of the distinctiveness of the computer virus reveals the flaws of the earlier models and a generic model SLBS is proposed. SLBS (Susceptible Latent Breaking out Susceptible) is a generic model.

Flaws of the earlier models:

The fundamental terminologies of the earlier models are

- A system can be referred as Internal or external is depending on whether the system in connected to the internet or not.
- A system/ device/computer is referred to as infected or uninfected based on whether there is any virus residing in the system or not.
- A system/ computer is considered as a host computer of a virus, if the virus has entered the system and residing in it.

The life cycle of the is calculated by the interval of time it enters the system and to the time it is removed from the system, this time is considered as the life time of a virus, the life time cannot be fixed rather it is affected by the variety of factors.

Stages of Virus:

The stages of virus has been classified into four categories they are

- Dormant
- Propagation
- Triggering
- Execution

Dormant:

The virus program has manages to access the target users computers or the software's, but the virus will be inactive and will not take any action during this stage.

Propagation:

The viruses place its matching copies of itself into the other programs or into other system areas on the disk. Each affected or infected program will contain the replica of the virus.

Triggering:

The virus's life cycle is when the virus completes its intended function, triggering phase the virus will starts its intended function.

Execution:

This is the main and actual work of the virus, where the consignment will be released; it can be much dangerous and destructive such as erasing the files on the disk, crashing the system etc.

Principle of computer virus:

The decisive goal of the intelligent computer virus is to devastate as many computer systems as possible, the virus will try to surreptitiously infect as many computers as possible before it finally breakout. Viruses undergo two successive phases they are

Latent phase: latent phase is the gap from the time the virus enters its host computer to the time accurately before it inflicts the harm on the host system.

Breaking out period: it is the gap between the time the virus begin to inflict damage to the time it is cleared out.

We discuss the two periods in additional that an infected system will be referred to as latent or breaking out depending on whether all virus residing in it are in their latent periods or at least one residing in its breaking period.

A familiar flaw model with E section:

In few of the biological infectious diseases an infected individual person may understand or experience a meticulous period of time named as the incubation or exposure period before the stage of infectivity. So the epidemic models should have individual E section. Few of the epidemic models of the computer virus were recognized by borrowing biological epidemic model with E section. Involving the previous hypothesis that some of the infected computers posses no kind of infectivity.

The most outstanding characteristics shown by all computer virus is their infectivity, on one side, once it is infected with a slight defined virus, a computer will have infectivity, because these infected computer can infect other computers when it shares resources between the other like sharing of resources, files, infected data's or attachments, sending E mail , transmitting infected files. On the other side once a computer system is infected with worms may posses' serious vulnerabilities. Therefore in the current scenario there exists no infected computer systems at all, that doesn't have any kind of infectivity, and equivalently there exists no exposed computer systems, that a rational epidemic model of the computer virus must have an E section.

The SLBS – A standard model:

We aim to put forward a standard epidemic model of computer virus based on the earlier discussions all internal computers can be classified into three groups

- Uninfected Internal Computer
- Latent Internal Computer
- Breaking out Internal computer

The entire three internal computers can be named as S, L, and B correspondingly.

All the External computers are also categorized into three groups

- Uninfected External Computer
- Latent External Computer
- Breaking out External Computer

The entire three external computers can be named as S*, L* and B* correspondingly.

We can denote the computers as S (t), L (t) and B (t) with a time t.

Let us enforce some hypothesis like

- The Internet is connected completely, so that all the internal computers can equally possible to be accessed by the other internal computers.
- S* (Uninfected External Computers) computers are connected to the internet at a unvarying rate r1 while L* at r2; i.e., r=r1+r2.
- Every Internal computer can be detached from the internet with an unvarying probability p1.
- Due to the outbreak of the viruses every B computer system is detached from the internet with an unvarying probability p2.
- Due to the get in touch with the infected removable storage Medias or devices, every S computer is infected with a probability p3.
- Due to the outbreak of the viruses every L computer systems becomes a B computer system with a probability p4.
- Due to the get in touch with L or the B computer system at every time t every S computer system becomes L computer system with the function f (L (t) + B (t)).
- Every B computer system is healed with an unvarying probability y1, L computer is healed with y2 and the B computer is partially healed i.e., an L computer with an unvarying probability y3.

Based on the collection of these hypotheses the corresponding SLBS standard model can be formulated to find the best solutions for the problem raised in the previous epidemic models.

Judging the Delay Terms:

There are mainly three possible delay factors that have prominent influence on the spreading of the computer virus.

- Due to the cost and time needed to create computer viruses, there is a wait or delay from the time where the B computer is cured and to the time again this computer gets infected.
- Due to the inherent latent periods a computer virus there will always be a delay from the time the S system get infected to the time the computer breaks out.
- Due to the cost and the time needed to develop the ne patches there will always be a delay in the time in the L computer breaks out to the time the computer gets cured.

So we do not suggest the SLBS models with the collaboration with the delay models as there may be chance of questions may arise like is it necessary to incorporate delay terms in the standard SLBS models. So we are not going to collaborate or incorporate the standard SLBS models with the delay models.

Conclusion:

By studying and investigating about the characteristics of computer viruses, we identified the problems or flaws of the previous epidemic models of the viruses. On this basis we proposed a standard epidemic models SLBS and few generalizations have been suggested.

This model is the only timeline solutions for the problems, great models with so many good parameters have to be investigated and yet to be identified. The SLBS is based on the fully connected network and it is highly rewarded to study the model properties on scale free networks. The research is opened to study about the computer virus study on scale free network with Biological epidemical models of virus.

REFERENCES:

[1]. J.O.kephart and S.R White, " Directed graph epidemiological models of computer viruses," in proceedings of the IEEE computer society symposium on Research in Security and privacy, May 1991.

[2]. P. Szov, "The Art of computer Virus Research and defence, AddisoWesley, 2005.

[3]. W. H Murray "The Application of Epidemiology to Computer viruses, "Computers and Security", Vol 7, no 2, pp 139-145, 1998.

[4]. E. Ravasz and A.L Barabasi, "Statistical mechanics of computer network, " Reviews of Modern Physics, Vol 7, 2002.

Sudeesh Kumar G. "Epidemiological Imitation of Computer Virus." *International Journal of Engineering Research and Applications (IJERA*), vol.10 (04), 2020, pp 50-52.