Worm penetration from desktop to mobile

Ankur Singh Bist*, Dr. Anuj Sharma*

*PHD Scholar SVU Gajraula, SVU Gajraula

Abstract: - Complexity of network applications has enhanced the problem of computer worms. At the same time the advancement in technology has given rise to evolution of portable mobile devices. It has become the danger point of day today activities like mails, mobile banking etc. Malware designer are also observing the same trend, due to the same reason lot of mobile malwares have arisen. This paper includes the discussion about penetration of malwares especially worms from desktop to mobile.

Keywords: - Mobile malware, Detection techniques, Unsolvable problems, Feature selection.

Introduction

Advancements in computer science and communications have made life easier in various ways. Internet banking, mobile banking, data storage at cloud etc. have added new dimensions in life of common man. Social networking like facebook etc. connects the people. Nothing is one sided in this world, every advancement have certain pros and cons. Current framework of discussed technology is susceptible with threat of malware like viruses, worms etc [2] [3] [4].

Computer virus infections have imposed significant financial loss. Antivirus technology is also upgrading to fight against latest malware. Signature detection methods do not work with perfection since there are zero day attacks [1].

The evolution of detection techniques involves the concept of static analysis, dynamic analysis and hybrid analysis. Machine learning techniques like neural networks, Hidden markov models are widely used to detect metamorphic malwares [5] [6] [7] [8]. Following figures depicts the recent trend of virus propagation.

Types of Malware

Software that contains instructions causing harmful impact is called malware. Based on different factors like behavior, evolution etc. malware can be categorized. Figure 1 depicts simple classification of malware. The first reflection of malwares was found in viruses. Fred Cohen described computer virus as a
program that causes effect using its property of self-replication. The basic definition of viral set can be defined as:-

For all Turing machines M and all non empty sets of Turing programs V the pair ( M,V) is a viral set if and only if for each virus v belongs to V, for all histories of the machine M we have:-

For all the instance t belongs to N and cells j of M if

1. The tape head is in front of cell j at time instant t
2. M is in its initial state at time instant t
3. The tape cells starting at index j holds the virus v, then, there exists a virus v1 belongs to V at time instant t1>t and at index j1 such that
   a. Index j1 is far enough from v position
   b. The tape cells starting at index j1 hold the virus v1
   c. At some time instant t2 such that t<t2<t1, v1 is written by M.

Figure4: Malware threat distribution

Worm can be defined as a program that can propagate by itself to other computers. Spying is a malicious program that steals information from one machine and transfers this information to the hacker. Trojan horse attracts the user by reflecting some useful functionality and finally causes harm. Rootkits are the collection of tools used by hacker after taking control over machine. It can be classified as user mode root kits and kernel mode root kits. Botnet can be defined as a collection of bots which runs on zombie machines controlled by attacker. Our main purpose is to focus on metamorphic viruses. Computer viruses can be classified into different categories. Boot virus replicates into one or multiple form into next generation and takes benefit of boot sequence of computer. Native viruses are 32 bit windows viruses and retrieve API to replicate. ELF (executable and linking format) viruses on UNIX generally recognized by internal structure and do not have extension in files. Macro viruses copy itself for fulfilling the purpose of attacking global template. Prepending viruses uses the technique of virus code insertion in front of host program. Cavity viruses use the technique of overwriting instead of increasing the size of object. Tunneling viruses try to control chain of interrupts call. Most of tunneling viruses belongs to the category of memory resident. Armored viruses contain function set designed in such manner that it becomes difficult to analyze them [10-19]. The main theme is to survive without being detected by antivirus software. Encrypted viruses modify their content with the help of encryption techniques due to this it becomes critical to analyze and detect these type of viruses. Oligomorphic viruses use the technique of decryptor code substitution in successive generations. Signature detection becomes impractical to detect these types of viruses. Polymorphic viruses are identical to Oligomorphic viruses but the difference is that polymorphic viruses have the capability to produce infinite decryptors. Next category is metamorphic viruses, let’s take deeper look to understand it.

Function structure of worm contains main body function and auxiliary function. Main body contains information collection module, probe module, attack module and self propagation module. Auxiliary function contains concealment module, crash module, communication module, remote control module and automatic updating module. There are different techniques adapted by worm to target the host. It can be classified as follows:-
1. Selective random scan
2. Sequential scan
3. Hit list scan
4. Routable scan
5. DNS scan
6. Divide conquer scan

In order to identify the worm spread and to estimate the prediction of worm propagation various models are designed:

1. Simple epidemic model
2. Kermack-McKendrick model
3. Susceptible Infectious Susceptible model
4. Two factor model
5. Worm anti-worm model

There are various qualitative trends with respect to computer worm.

1. Commoditization
2. Convergence
3. Social Engineering
4. Additional propagation vectors
5. Speed of propagation
6. Countermeasure awareness

There are various machine learning techniques like ANN, Decision tree etc. are used to detect computer worms. Software like Vtrace is widely used to collect features for worm detection. Feature selection is crucial step in order to make detection effective and fast. There are various techniques for the same.

1. Chi-Square
2. Gain Ratio
3. Relief

Android Malware

Figure 5: Android architecture

APK auditor is permission based android malware system. APK Auditor consist of three main components.

1. An android client
2. A signature database
3. A central server

Figure 6: APK Auditor software architecture

There are various assessment, analysis and detection tools. Some of them are as follows.

1. Androguard
2. Andromaly
3. AndroSimilar
4. Andrubis
5. APKInspector
6. Aurasium
7. CopperDroid
8. TaintDroid
9. Crowdroid
10. DroidBox
11. DroidScope
12. Drozer
13. JEB
14. Kirin

Classification Parameters

1. Confusion Matrix- In predictive analytics, a table called a confusion matrix, is a table with two rows and two columns that signifies the number of false negatives, false positives, true positives, and true negatives.
   a.) True Positive (TP)- It defines how correctly an algorithm is in identifying a malware as virus.
   b.) False Positive (FP)- It is the number of mistakenly classified instances as positive.
   c.) True Negative (TN)- It is the number of correctly classified instances as negative.
   d.) False Negative (FN)- It is the number of mistakenly classified instances as negative.

2. Accuracy= \( \frac{TP+TN}{TP+TN+FP+FN} \)
3. Precision= \( \frac{TP}{TP+FP} \)
4. Recall= \( \frac{TP}{TP+FN} \)
5. F-measure= \( \frac{2 \times \text{precision} \times \text{recall}}{\text{precision} + \text{recall}} \)
6. ROC- Receiver Operating Characteristic (ROC) curve defines how a identification rate change as the internal threshold varies to produce more or fewer false alarm.

Conclusion-
In this paper we discussed about computer worms and their propagation scenario. With this a shift of malware attack from desktop to mobile devices is shown. Among all mobile OS, almost 70% market is covered by android, the same scenario reflects in the case of mobile malware attack in term of propagation. This survey will be helpful for all working in the field of computer virology.

Acknowledgement
I want to thank all who directly or indirectly supported in this work. I want to extend my special thanks to Dr. Anuj Sharma for continuous support.

References
10. Sharma, Rudranshu, Ankur Singh Bist, and Vikas Kumar. "INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY EXTREME LEARNING MACHINE."


17. Mehta, Pankaj, et al. "Image Classification using NPR and Comparison of Classification Results."

18. Das, Purushottam, Shambhu Prasad Sah, and Ankur Singh Bist. "INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY RECENT TRENDS IN XOR PROBLEM."
