Malwares Detection and Prevention Using Set Theory

Suchitra Choudhary[1], Khaleel Ahmad[2], Jayant Shekhar[3]

CSE & IT Deptt. Swami Vivekananda Subharti University, Meerut, U.P., India

Abstract

Dependence of electronic devices (viz. Computer, Laptop, Mobile etc.) is increasing exponentially, so large amount of data and information are stored on electronic devices. These electronic devices are interconnected in local, national and international networks, use and share a high number of various software programs. Individuals, corporations, hospitals, communication networks, authorities among others are totally dependent on accessibility of the data and information stored. Malwares have different objectives and different techniques to corrupt the database or dump the system. In this paper, we propose the novel model for malware detection and prevention for security purpose. The proposed model detects the malware and prevents the electronic devices from the malwares which can destroy or delete the data from electronic devices. In this paper, we propose an algorithm for the detection and prevention; we use set theory for detection and prevention the malwares.

Keyword: Malwares, Detection, Prevention, Set Theory

1. Introduction

Forensic Science is the technique to identify that criminal who's involved in illegal action in the organization [1]. Forensic science is a very broad term. It covers any aspect of science which may be of use in a court room [2]. It is the application of a broad spectrum of science to answer questions of

interest to legal system. Malware detection and prevention is also a part of forensic science [3].

Malwares (malicious program/ rogue code) are software program capable of reproducing themselves and usually capable of causing unintended hidden logic which many times lead to great harms to files or other program on the system and network [4]. Malware or malicious software is designed to damage a computer system without the owner's informed [5].

There are two types of malware programs:

There are two types of malware programs:

(i) Need host program (ii) No need host program

(i) Host need program:

Programs that must require a host program. These programs cannot exit by themselves; they need some application, utility or some application program [6].

(ii) No need host program:

Program does not require host program. These programs can exit independently [7].

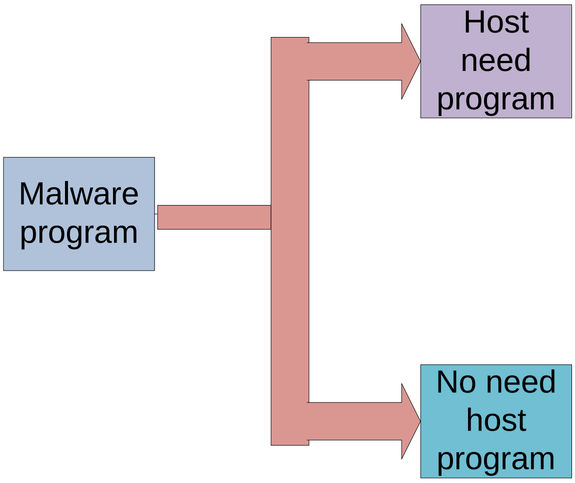

Figure: 1 Types of Malwares

2. Related Work

As dependency on Internet and electronic devices such as computer, laptop and mobile extended [8]. There are many disadvantages such as lack of security, User ID theft, Leakage of information, etc [9]. There are many people who are performing their work in this field such as Gursimran Kaur, Bharti Nagpal research topic is Malware Analysis & its Application to Digital Forensic [10]. First, authors studied about how to analyze the malwares on the system for digital investigation. Secondly, authors introduced malware analysis tools.

3. Proposed Model

In this paper, we proposed the model for malware detection and prevention. By this model, the system first detects the malwares and then prevents the system from the malwares. In this paper, we used set theory for detecting and preventing the malwares.

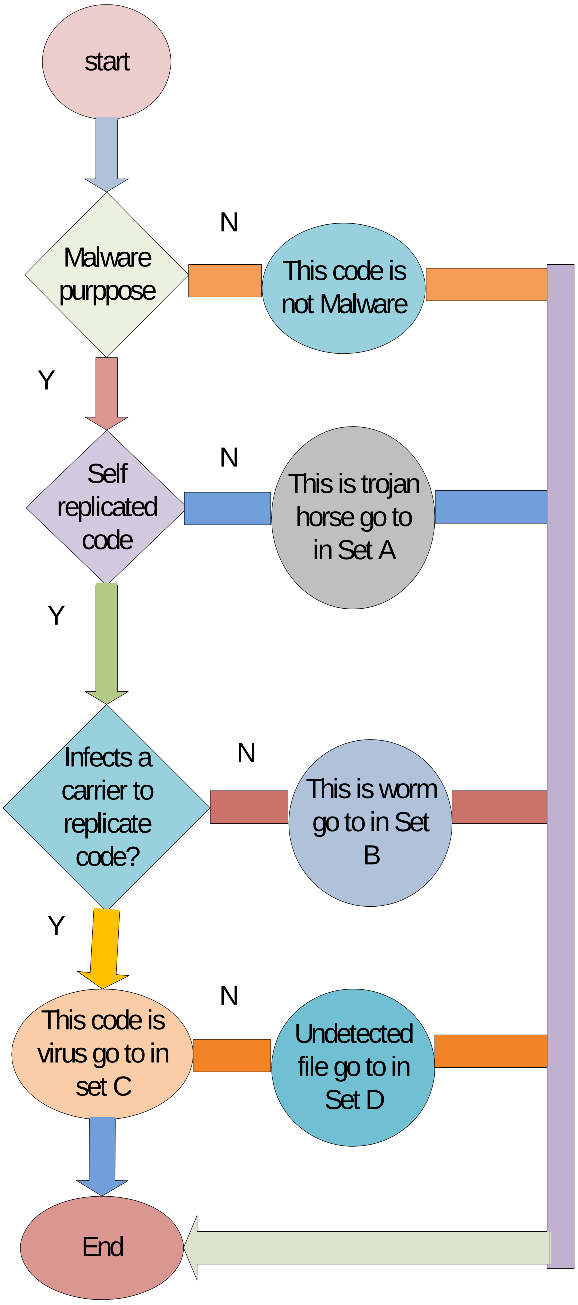
start
Malware purppose
N
This code is not Malware
Y
Self replicated code
N
This is trojan horse go to in Set A
Y
Infects a carrier to replicate code?
N
This is worm go to in Set B
Y
This code is virus go to in set C
N
Undetected file go to in Set D
End

Figure: 2 Malware Detection Model

Algorithm:

```
1:  Start
2: IF 'Malware Purpose'
3: Then IF 'Self Replicated Code'
4: Then IF 'Infects a carrier to replicate'
5: Then 'This code is virus' GOTO Step-10
6: ELSE 'This code is worm' GOTO Step –10
7: ELSE 'This code is Trojan' GOTO Step-10
8: ELSE 'There is no malware code' GOTO Step-10
9: IF 'Undetected File' GOTO Step-10
10: END
```

When the malware detection code executes then it will check the file is the malware or not as shown in figure 2. If the file is not malware then it will show that there is no malware code. If the file is malware then it will check the code that is self replicated or not. As in figure 2 described, if the code is not self replicated code then this is Trojan and send the code in Set A. If the code is self replicated then check it will infects a carrier to replicate or not. If code is not infects a carrier to replicate then this worm and send in Set B. If the code is infects a carrier to replicate then this is virus and send in Set C. If the file is not detected then the file will send in Set D as described in figure 2.

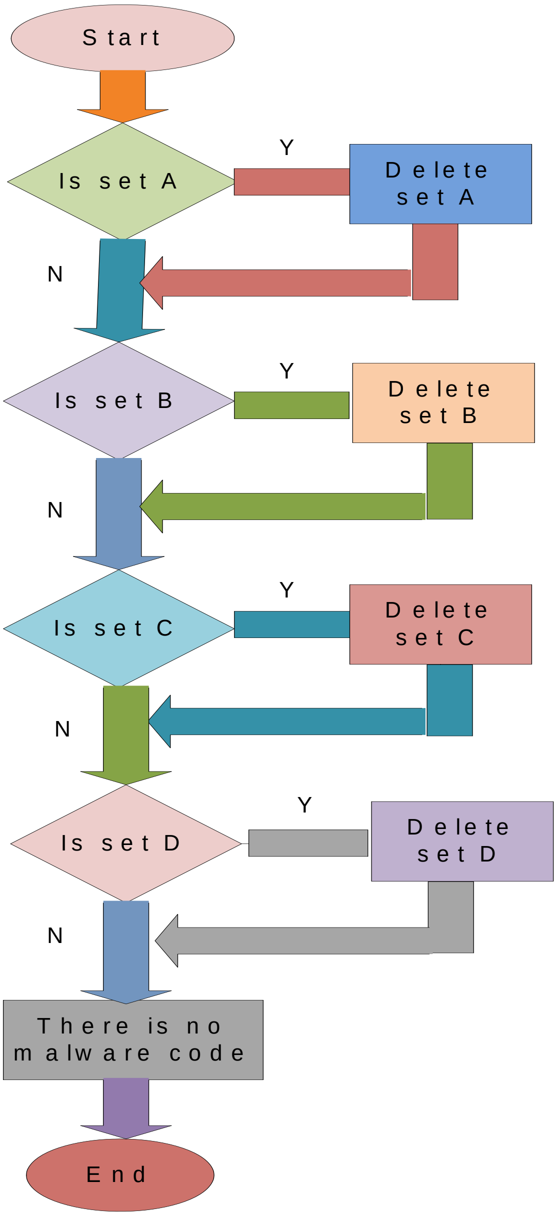

Figure: 3 Malware Prevention Model

Algorithm:

```
Start
IF ‘Set A’
Then ‘Delete Set A’
Else IF ‘Set B’
Then ‘Delete Set B’
Else IF ‘Set C’
Then ‘Delete Set C’
Else IF ‘Set D’
Then ‘Delete Set D’
Else ‘There is Malware Code’
End
```

After detecting the malwares, the malware prevention model will work. The malware prevention model will work as shown in figure 3. The model will check, if there is Set A then the model will delete the Set A, otherwise the model will execute for the next step. If the model finds the Set B then it will delete the Set B and now check for Set C, if the model will find Set C then the model will delete the Set C, now the model will check for Set D, if there is exits Set D then the Set D will be deleted, otherwise give the message that there is no malwares code as shown in figure 3.

Conclusion:

In this paper, we are analyzed present dependency of electronic device such as computer, laptop, mobile etc. increases in various fields viz. corporate field, personal etc. As the demand of security tools increased because the possibility of attack of malwares are increased. So, in this paper we design the malware detection and prevention model for tight security. We used Set Theory for the malware detection and prevention.

References:

[1] Masood, S. G. (2004). Malware Analysis for Administrators. Retrieved 17 March, 2007 from http://www.securityfocus.com/infocus/1780.

[2] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee. BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation. In USENIX Security Symposium, 2007.

[3] U. Bayer, I. Habibi, D. Balzarotti, E. Kirda, and C. Kruegel. A View on Current Malware Behaviors. In 2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET), Boston, MA, April 2009.

[4] EICAR — The Anti-Virus or Anti-Malware Test File.http://www.eicar.org/antivirus test file.htm.

[5] Virus Total. http://www.virustotal.com.

[6] Kolbitsch, C., et al., “Effective and Efficient Malware Detection at the End Host”, In 18th Conference on USENIX Security Symposium, 2009, p. 351-366.

[7] Yin, H., et al., “Panorama: Capturing System-wide Information Flow for Malware Detection and Analysis”, In 14th ACM Conference on Computer and Communications Security, 2007, p. 116-127.

[8] D. Du, S. Narasimhan, R. S. Chakraborty, and S. Bhunia, “Self-referencing: a scalable side-channel approach for hardware trojan detection,” in 12th International Conference on Cryptographic Hardware and Embedded Systems (CHES). Springer-Verlag, 2010.

[9] Kinder, J., Katzenbeisser, S., Schallhart, C., Veith, H.: Detecting Malicious Code by Model

[10] Checking. In: Julisch, K., Kruegel, C. (eds.) DIMVA 2005. LNCS, vol. 3548, pp. 174–187, Springer, Heidelberg (2005).

[11] Smith, S., & Quist, D. (2006). Hacking Malware: Offense is the new Defense. Retrieved July 24, 2007 fromhttp://www.offensivecomputing.net/dc14/valsmith__dquist_hacking_malware_us06.pdf.