ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Detection of Logic Bombs

Ankur Singh Bist
Quantum Global Campus, Roorkee, India
ankur1990bist@gmail.com

Abstract

Computer viruses are big threat to computer world; researchers doing work in this area have made various efforts in the direction of classification and detection methods of these viruses. Graph mining, system call arrangement and CFG analysis are some latest research activities in this field. The computability theory and the semi computable functions are quite important in our context of analyzing malicious activities. A mathematical model like random access stored program machine with the association of attached background is used by Ferenc Leitold while explaining modeling of viruses in his paper. Computer viruses like polymorphic viruses and metamorphic viruses use more efficient techniques for their evolution so it is required to use strong models for understanding their evolution and then apply detection followed by the process of removal. Code Emulation is one of the strongest ways to analyze computer viruses but the anti-emulation activities made by virus designers are also active. This paper involves the study of logic bombs.

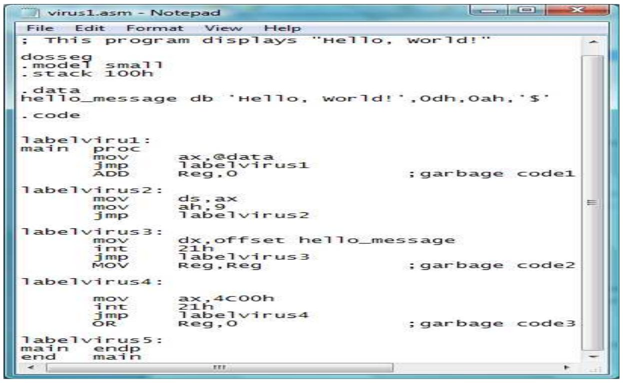
Keywords: logic bombs, Malicious Codes.

Introduction

There are various processes that have been used in the direction of classification of worms from normal files that will finally lead to worm detection. Machine learning techniques are widely used in this direction. As statistics says that the attacks of malicious codes are increasing day by day so there is requirement of strong techniques that can be used for their detection. Worm designers or in total we can say malicious code designers use lot of techniques that are difficult to analyse and detect. The static methods also seems not to work in the case where every time there are rapid dynamicity from attacker side so now a days main focus is going towards the methods that are dynamic and are able to detect zero day worms .

The rise in the malicious threats like computer worms activities are required to be handled and observed strongly to make certain defence that can stand as a saviour of security domain. Other types of malware are:

1. Viruses
2. Trojan horse
3. Botnets
4. Adware
5. Spyware



```
; This program displays "Hello, world!"

dosseg
.model small
.stack 100h

.data
hello_message db 'Hello, world!',0dh,0ah,'$'

.code

labelviru1:
main   proc
       mov     ax,@data
       jmp     labelvirus1
       ADD     Reg,0                    ;garbage code1

labelvirus2:
       mov     ds,ax
       mov     ah,9
       jmp     labelvirus2

labelvirus3:
       mov     dx,offset hello_message
       int     21h
       jmp     labelvirus3
       MOV     Reg,Reg                  ;garbage code2

labelvirus4:

       mov     ax,4C00h
       int     21h
       jmp     labelvirus4
       OR      Reg,0                    ;garbage code3

labelvirus5:
main   endp
end    main
```

Figure1. Assembly file of virus

The mutating behaviour of metamorphic viruses is due to their adoption of code obfuscation techniques.

a) Dead code insertion
b) Variable Renaming
c) Break and join transformation
d) Expression reshaping
e) Statement reordering

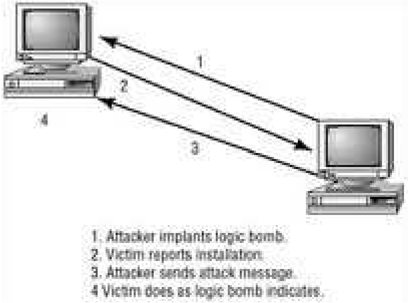

1
2
3
4
1. Attacker implants logic bomb.
2. Victim reports installation.
3. Attacker sends attack message.
4 Victim does as logic bomb indicates.

Figure 2: Logic Bomb

In year 2000, Tony Xiaotong, explained before a jury was accused of putting a logic bomb during his employment as a programmer and securities trader at Deutsche Morgan Grenfell. The bomb, kept in 1996, had an activation date of July 20, 2000, but was discovered by other programmers in the organization. Removing and cleaning up after the bomb allegedly took much time.

In year 2003 Yung-Hsun Lin, also known as Andy Lin, changed code on a server at Medco Health Solutions Inc. Fair Lawn, New Jersey headquarters, where he was employed as an administrator of Unix, creating a logic bomb set to go off on his birthday in 2004. It did not work due to error in programming, so Lin make correction in the error and reset it to go off on his next birthday, but it was found and disabled by a Medco computer systems administrator a few months before the activation date.

Logic Bomb and their Detection Schemes

A logic bomb can be defined as a program intentionally inserted into a software system that will put a malicious function when certain conditions are found. For example, a programmer may hide a program that starts updating files (such as a salary-update database trigger), should they ever be fired from the company.

What does *Logic Bomb* mean? A logic bomb is a malicious piece of code timed to make abnormality at a certain point in time, but is not active until that point comes. A set trigger, such as a preprogrammed date and time, make activation of logic bomb. Once activated, a logic bomb implements a malicious code that causes harmful activities in computer. A logic bomb's application programming points can also involve other variables such that the bomb is activated after a specific number of database entries. However, computer virology researchers believe that certain gaps of action may start a logic bomb as well, and these types of logic bombs may cause the typical harm to computers. A logic bomb may be implemented by one that is trying to sabotage a database when they are fairly certain they won't be present to experience the effects, such as full database deletion. In these instances, logic bombs are programmed to exact sabotage task.

Techopedia (defines): Logic Bomb

Logic bombs are normally used for harmful purposes, but they can also be used as a timer to stop a consumer from using certain software past a trial basis. In this case, unless the consumer ends up purchasing the software at the end of the free trial, a trial bomb will deactivate the program. If the vendor wants to be particularly nasty, it can program the trial bomb so that it takes other data along with it, not just the program data.

Logic bombs can be extremely harmful should they initiate cyber wars, something that is related to former White House counterterrorism expert, Richard Clarke. Clarke explains his concerns about cyber war in his book named "Cyber War: The Next Threat to National Security and What to do about it." In this book, Clarke explains that the U.S. is very vulnerable to this type of attack because its infrastructure is much dependent on computer networks in comparison with modern countries. Author cautions that malicious code designers could detonate logic bombs and all but shut down urban America's transit and banking systems. In year 2009, the Pentagon apparently heeded author's warning when it designed the U.S. Cyber Command. As reassuring as this may be, civilian IT professionals have neglected to enlist cyber war defense technologies to a big extent.

Software that is inherently malicious, such as viruses, worms and Trojan horse, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to achieve growth and spread before being identified. Some viruses attack their host systems on specific dates, such as 1 January or Christmas Day. Trojans that activate on certain dates are often called "time bombs". To fulfill the criteria for logic bomb, the payload should be unwanted and unknown to the user of the software. For example, some programs with code that disables certain functionality after a specific time are not normally regarded as logic bombs.

Some logic bombs can be identified and eliminated before they execute through a periodic scan of all files, including compressed files, with an up-to-date anti-virus program. For best results, the auto-protect and e-mail screening functions of the anti-virus engine should be activated by the computer user whenever the machine is connected to web. In a network, each computer should have separate protection schedule, in addition to whatever protection is provided by the network administrator. Unfortunately, even this precaution does not cause complete security. COTS software is used for dynamic analysis of backdoors, Trojan horses, time bombs, etc. These types of attack are not identified by standard virus detection engines, which are essentially the only commercially available tools that use directly binaries for identification. The complexity of a real time-bomb and hopefully of all types of malicious actions will be reduced by using dynamic analysis techniques. Automated tool to detect malicious actions in all their forms are designed by researchers. Dynamic analysis techniques can be used to overcome the inadequacy of the static methods. An environment for detecting many types of malicious code, including computer viruses, Trojan horses, and time/logic bombs, is proposed by researchers in recent years. The malicious code test bed (MCT) is based upon both static and dynamic analysis tools developed at the University of California, which have been shown its efficient behaviour against certain types of malicious code. The test bed extends the usefulness of available tools by using them in a complementary fashion to detect more general cases of malicious code. Perhaps more importantly, the MCT allows administrators and security analysts to check a program before installation, thereby avoiding any damage a malicious program might inflict. Using the code emulation techniques or by using virtual environment logic- bombs can be detected. Their presence can be checked by giving certain specific inputs to them in virtual environment it is done to reveal their behaviour. Simulation of time clock in virtual environment is another method for their detection.

Conclusion

This paper discusses about basic outline of logic bombs and their detection by using different techniques. The methods discussed are being used for solving different problems of this domain. This study will be helpful for researchers working in the field of computer virology.

References

[1] www.wikipedia.com.

[2] http://www.techopedia.com/definition/4010/logic-bomb.

[3] Salois, Martin, and Robert Charpentier. Dynamic detection of malicious codes in COTS software. DEFENCE RESEARCH ESTABLISHMENT VALCARTIER (QUEBEC), 2000.

[4] Lo, R., et al. "Towards a testbed for malicious code detection." COMPCON Spring'91. Digest of Papers. IEEE, 1991.

[5] Bist, Ankur Singh. "Classification and identification of Malicious codes."