ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Spyware Detection Techniques

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 spywares.

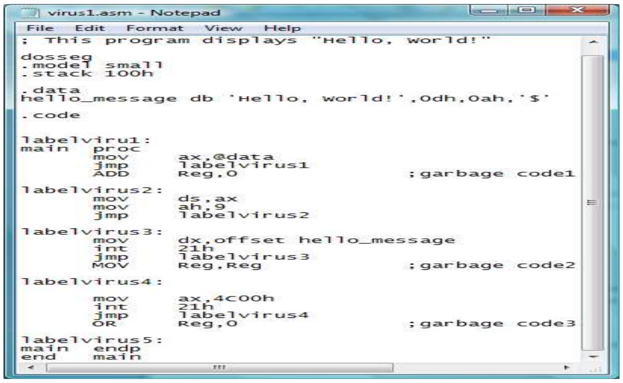
Keywords: Spyware, Browser Helper Object.

Introduction

There are various processes that have been used in the direction of classification of computer viruses from normal files that will finally lead to their 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. 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 on towards the methods that are dynamic and are able to detect zero day computer viruses.

The rise in the malicious threats like computer viruses 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. Worms
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

Spyware Activities

Spyware is a malicious program that gathers information about a person or organization without their knowledge and that may send the theft information to another person or entity without the consumer's consent, or that makes control over a computer without the consumer's knowledge.

Spyware can be categorized into four types:

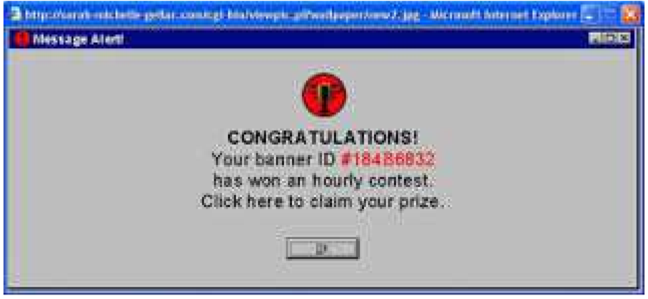
1. System monitors
2. Trojans
3. Adware
4. Tracking cookies

Spyware mainly fulfills following purposes-

1. Tracking and storing internet users' activities on the web.
2. Serving up pop-up ads to users on internet.

Whenever spyware is used for harmful purposes, its presence is typically hidden from the user and it is not easy to detect their presence. Some spyware, such as key loggers, may be installed by the proprietor of a shared, corporate, or public computer purposely so that they could track the activities of user.

While the term *spyware* indicates software that monitors a user's movements, the functions of spyware can extend beyond simple monitoring. Spyware can analyze and collect almost any type of data, as well as personal information like Internet surfing habits, user logins, password information and bank or credit account information. Spyware can also obstruct with user control of a computer by installing additional software or redirecting Web browsers. Some spyware can modify computer settings, which can slow down speed of Internet connection. Spyware can also make un-authorized changes in browser settings, or changes to software settings. Following picture indicates situation regarding spyware.


http://sarah-michelle-gellar.com/cgi-bin/viewpic.pl?wallpaper/new7.jpg - Microsoft Internet Explorer
Message Alert!
OK

CONGRATULATIONS!
Your banner ID #18486832
has won an hourly contest.
Click here to claim your prize.

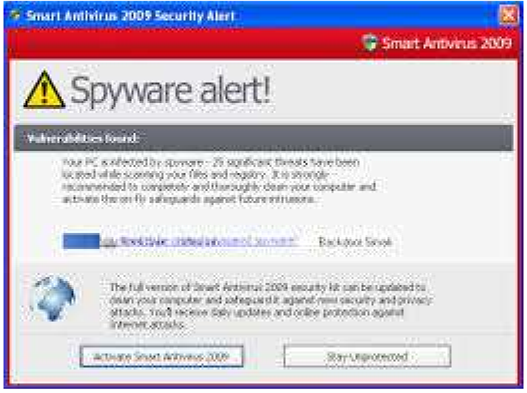
Sometimes, spyware is included along with benign software, and may come from a malicious source or website. In response to the emergence of spyware, computer virology researchers have come up. Running anti-spyware software has become a widely common part of computer security practices for computers, particularly those working in windows environment.

Spyware does not necessarily behave or spread in the same way as a virus or worm because infected computers generally do not attempt to transmit or copy the software to other systems. Instead, spyware installs itself on a computer by deceiving the user or by exploiting software vulnerabilities.

Spyware may try to deceive users by mixing itself with desirable software. Other common strategies are using a Trojan horse. Some spyware authors infect a system through protection holes in the Web browser or in other software. When the user navigates to a Web page controlled by the spyware writer, the page contains program which attacks the browser and forces the download and installation of spyware.

The installation of spyware normally involves Internet Explorer. The main reason is the popularity of internet explorer that has made it target of spywares. Its deep integration with the Windows environment makes it prone to attack into the Windows operating-system.

Internet Explorer also serves easy environment for spyware in the form of Browser Helper Objects, which modify the browser's behavior to add toolbars or to redirect traffic. Following picture depicts situation regarding spyware alert.


Smart Antivirus 2009 Security Alert
Smart Antivirus 2009
Activate Smart Antivirus 2009
Stay Unprotected

Spyware alert!

Vulnerabilities found:

Your PC is infected by spyware - 25 significant threats have been located while scanning your files and registry. It is strongly recommended to completely and thoroughly clean your computer and activate the on-fly safeguards against future intrusions.

[illegible] Backdoor.Small

The full version of Smart Antivirus 2009 security kit can be updated to clean your computer and safeguard it against new security and privacy attacks. You'll receive daily updates and online protection against Internet attacks.

With the growing popularity of anomaly detection systems, which is used to defend against zero-day attacks, a new class of threats have evolved where the attacker mimics legitimate activities to merge in and avoid detection. In literature authors have proposed a new system called Siren that injects crafted human input alongside legitimate user activity to handle these mimicry attacks. The crafted input is specially designed to trigger a known sequence of network requests, which Siren compares to the actual traffic. It then marks unforeseen messages as malicious. Using this technique, authors were able to detect ten spyware programs that were tested, many of which attempt to merge in with user activity. Another way to detect spyware presence is to look on the activities of browser helper object, if BHO (browser helper objects) are leaking sensitive information, and then it may confirm the presence of spywares. Malicious threats literature explains that Spyware is the latest epidemic security threat for Internet users. There are various types of spyware programs creating severe problems such as copying and sending important information, consuming CPU power, reducing offered bandwidth, irritating users with endless pop-ups, and monitoring users' computer usage. As spyware makes the Internet unsafe place and reduces user interest in online activities, Internet users stop purchasing at online stores is a consequence that clearly disrupts e-business.

Conclusion

This paper discusses about basic outline of malicious codes and especially spywares and their detection using different techniques. This study will be helpful for researchers working in the field of computer virology.

References

[1] www.wikipedia.com.

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

[3] Borders, Kevin, Xin Zhao, and Atul Prakash. "Siren: Catching evasive malware."Security and Privacy, 2006 IEEE Symposium on. IEEE, 2006.

[4] Lee, Younghwa, and Kenneth A. Kozar. "Investigating factors affecting the adoption of anti-spyware systems." Communications of the ACM 48.8 (2005): 72-77. Farrokh Mamaghani, (Associate Professor of Information Technology, Department of Management, St John Fisher College, Rochester, New York, USA)