Heuristic Analysis Approach for Malware Detection on Internet Banking

Gaurav Sharma, Utkarsh Mehta, Dilpreet Singh Sachdeva

Abstract— No field has been exempted from the effect of malware and internet banking is one of them, nowadays malware is a serious problem, malware is a big threat to internet banking.It has become a threat to users.Hence many researchers have made many detection techniques to lower and overcome this problem. Heuristic Analysis or Pro-Active Defense is one of the best ways to alleviate this problem but it also have some issues many times this technique was questioned by researchers about the proper working of this approach.In this paper we will work on Heuristic Analysis or Pro-Active Defense techniques with the help of Signature based mechanism. In previous time there were many techniques to attenuate this gigantic problem unfortunately; hackers were successful enough to crack today detection tools.

Index Terms— Heuristic analysis, Internet banking, Malware, Digital Signture.

1 Introduction

Malware is such a malicious code that constantly keeps on changing its form and is also capable of doing things without being seen.Malware has one more attribute which creates a problem in detectingthem,which is,they transfers to one's system without letting the user know that there is malware in his system.Internet banking is one of the major threat and malicious programmers often make the bank accounts their target to rob money from their accounts.The account owners don't even get to know that they have malwarein their systems,as a result of which,their personal information,account identification are being stolen without leaving any trail of suspect.

Many techniques are uses by these malicious programmers to create malware, that is the reason Heuristic Analysis or Pro-Active Defense or Signature based techniques will help in lessening the destruction caused by these attackers through malwares.

.

2 Uses of Malware

Today, malware is used for creating malicious code. It is through by the attackers to seek essential account information of the customers which includes account pin, account number etc.

Denial of service attacks:

When there are number of requests on an exacting served, speed of a server reduce to its lowest capacity and can even cause the server t shut down for some time.This is ideal time for the attackers to get into the system and do their work without giving any hint to the customer or admin of that particular page.Malicious programmers do this by sending large number of requests which isbeyond the holding capacity of that server.

3 Theft of Information

Stealing important data is what hackersdo.They steal the data and sometimes they also sell the information to make money.

BOT NET:

Bot is like a master computer which remotely controls the malicious code which is responsible for infecting the system from which secret information is extracted.Bot master controls all other bots remotely.The machines those are controlledby the bot master are called as the bot nets.

Now the question arises, how the bot master gets linked to the other bot net.This is done by sending spams or junk e-mail messages which may links to some infected website.

These web sites/webpages might secretly use a malware element using some other system which as a result gathers important information,for example credit/debit card number,pinetc.These details are now sent back to the malicious programmer or the attackerwho is now able to access the debit/credit cards by means of paying for merchandise on the web.

Today's internet banking security:

As it is said, everything has its advantage and disadvantage-making payments by means of credit/debit cards/internet banking cards has made our lives a lot easier,it also comes with someflaw in it.Oneproblem with the internet banking is its safety.E-Banking safety is usually to protect precious the account credentials of the customer from the malicious programmers of in other words attackers.This is why financial institutions need to continuously keep on changing their safety methods to protect by the attackers.Having a fully secured defense system should also be not that costly that the cost of making secure software of protecting the account information

- *Gaurav Sharma is currently working as Asst. Prof. in computer science engineeringdepartment in ITM, Gwalior, INDIA. gaurav0886@yahoo.com*
- *Utkarsh Mehta is currently pursuing bachelor degree program in computer science engineering in ITM, Gwalior, INDIA. utkarshmehta93@gmail.com.*
- *Dilpreet Singh Sachdeva is currently pursuing bachelor degree program in computer science engineering in ITM, Gwalior, INDIA. dilpreet2007@gmail.com*

may cost more than the money or they have in their organization. This is the main reason why mostly of the attackers don't try to get into bigger organization because they know that this bank will be having a very secure network protection and breaking into that will not be easier for them.Net banking is highly risky and is always exposed to some or the other attacks.

4 INTERNET BANKING FLAWS

The malware is supplied mostly by the methods for diminishing legitimate sites, after which utilization or social compositional methodologies to download, and deal with the real executable Shylock Dropper. The main traffic involving attacks had been carried out by the method of 'advertising', where the destructive system codes are present in promotional advertisements, which are present on commercial systems and several dependable and trustworthy websites. Nevertheless, the genuine Shylock representatives have supplement this lately, and have ataken a major step and procedure for most likely diminishing sites overseeing dated sorts including mainstream internet sites, like wordPress. Shylock Malware, also called Caphaw, is a Trojan of banking. It has co-ordinated with n number of measures that have been embraced by other these dangerous codes. This includes, positioning with a boot kit in a sequential manner to introduce a root-kit driver; then ending it with an extendable malware, which will be set to carry out adaptable 'man'in-the-web-browser' attacks.
The design for this finically supports the threats of cyber crime and credential theft. In deeper understanding—the start-up and working of the malware, with proper methods, thistechnique helps to remove the unclear coding from the malware code, to narrow down the search for the same. This method mentions that the code would go through the normalized and then it will be kept for match with a document current in the archive. If the code is same, it then transforms itself to the most recent signature and then kept aside in the store. Now taking in consideration an algorithm which is called as signature which is produced from from a text derived from a text.It main function is to uniquely identify aVirus. It depends on various types. There are very many scanners available. Depending upon the scanner which is being used .It can be stationary hash which is a calculated numerical value or a small piece ofinformation. This is its simplest form. The algorithm also depends upon the behavior.one unique signature can be consistent among very many viruses .A virus signature is a viral code which easily spreads from one place to another. Now, to identify the viruses or any malwares. What antivirus does is, it compares the proportion of the file with the list of signatures which is then useful in removing viruses.

5 CONCLUSION

In this research paper we have studied the malware,its effect,how the malicious programmers uses them to enter the system and steal important information like account credentials and PIN number of credit/Debit cards.

Malware is very dangerous and banking systems should make their systems very secure to prevent their system from the attacks of a malware.Hence, some really beneficial methods are provided in the paper.I hope,this paper of mine will prove to be helpful withthe security issues and effects of malware.

ACKNOWLEDGMENT

We are thankfull to ITM Gwalior to providing us facilities and kind support throughout research. I am also thankfull to almighty.

REFERENCES

[1] J. Reavis, "The Ongoing Malware Threat", Symantec White Paper, 2012.

[2] Standard Chartered Bank, "Standard Chartered Advisory Alert", April 2013.

[3] H. S. Dalla and Geeta, "Cyber Crimes: A Threat to Persons, Property, Government and Societies", International Journal of Advanced Research in Computer Science & Software Engineering (IJARCSSE), Volume 3, Issue 5, May 2013..

[4] K. Mathur and S. Hiranwal, "A Survey on Techniques in Detection and Analyzing Malware Executables", International Journal of Advanced Research in Computer Science & Software Engineering (IJARCSSE), Volume 3, Issue 4, April 2013.

[5] Z. A. Reis, S. Gülseçenb and B. Bayrakdarc, "To Develop an Education System for Secure Internet Banking: GIBES", Science Direct, 2011..

[6] Damballa Labs, "DGAs in the Hands of Cyber Criminals - Examining the state of the art in malware evasion techniques", Damballa, 2012

[7] Uppal, V. Mehra and V. Verma, "Basic survey on Malware Analysis Tools and Techniques", International Journal on Computational Sciences & Applications, International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1, February 2014.

[8] M. Christodorescu, J. Kinder, S. Jha and S. K. H. Veith, "Malware Normalization", Published in conference at University of Wisconsin, Technische Universitat Munchen, 2012.

[9] M. Christodorescu and S. Jha, "Testing Malware Detectors", International Symposium on Software Testing and Analysis, ISSTA'04, Boston, USA.

[10] R. Bhatnagar, M. K. Ansari, S. Bhatnagar and H. Barik, "Expert Anti-Malware Detection System", International Journal of Soft Computing and Engineering, ISSN: 2231-2307, Volume-2, Issue-5, November 2012.