International Journal of Grid and Distributed Computing
Vol. 9, No. 6 (2016), pp.63-70
http://dx.doi.org/10.14257/ijgdc.2016.9.6.07

A Study and Model to protect Sophisticated Eurograbber attack

Md Nadeem Ahmed [1] and Prof (Dr)Mohd Hussain [2]

[1]*Research Scholar,*
[2]*Professor*
[1]*Department of Computer Science,IFTM University, India*
[2]*MGMIT Lucknow, india*
[1]*mdnadeemahmed.86@gmail.com,* [2]*mohd.husain90@gmail.com*

Abstract

Smartphone now a days are very common to everyone and it is widely accepted. According to eMarketer [4] more than 2.56 billion people will use Smartphone by 2018 and up to 2015 more than one fourth of the world population is using Smartphone. It is widely because of its multiple functionality which allow us to accomplish more than what we expect. Apart from basic feature it is used for e banking, web browsing etc. Almost all restricted or confidential data is stored in Smartphone which leads to sophisticated attack like Eurograbber which happens through mobile botnet installation. This attack even fails the most successful two factor authentication which is worldwide accepted by banks. The Botnet differentiate itself from common other mobile virus because its infected system is capable to create a link with C&C (command and control centre) controlled by bot master. In this paper we will discuss about Eurograbber attack , the problem scenario and the model to prevent this sophisticated attack.

Keyword: *mobile botnet, cybersSecurity, Eurograbber, mobile malware, dropzone;*

1. Introduction

This is all about an intelligent and sophisticated Cyber attack which stolen approximately over 36 million euro across the Europe and attacked around 30,000 bank consumer. Initially the attack is reported in Italy and promptly more than 10,000 customer from Germany , Holland and Spain has been identified. The bank customer is not aware that they have been attacked with the ZITMO(Zeus-In-The-Mobile Trojan) and their e banking session has been hacked and amount stolen. Versafe and Check Point Software Technologies has recognized and named this attack as " Eurograbber ".There are multiple steps involved to infect the mobile (Blackberry and Android platforms)and desktop machine of the user and once mobile Trojan successfully installed on both machines the session of the e commerce application user were tracked by the hacker and even the most successful second factor authentication is failed in this and it is controlled and used by the hacker to validate the illegal transaction.

The hazard and attack on Smartphone possible is different forms such as worms, viruses, torjans and mobile botnet[1] but mobile botnet is most threatening as it create momentous hazard to phones and mobile network[2],[3]. A Machine became a bot once a software which get installed into machine which happens during the web browsing or alternatively from responding to the phishing email, DDos,information stealing or click fraud which tempts the user to click on the spurious url. Once it installed it starts the communication to command and control centre (C&C) server which administer it to execute further. This is the initial phase of attack and whenever the user login to his or her bank account the the customized software (Zeus, SpyEye or CarBerp Trojan) identify the login which prompt the next stage of attack.The data which is collected is stored in Database which may be used in future for eurograbber attack. Attacker apply various

ISSN: 2005-4262 IJGDC

domain names and server in order to circumvent detection and some of them were proxy server in order to make complex detection. If detection is on radar the hacker could rapidly change their infrastructure.

A Botnet is group of infected machine (bots) communicating to commands from server(C & C server) that perform as a assignation technique for commands from botmaster (Human controller). The bot of botnet bridge to command and control centre which depends on the instructions of botmaster[5] . The command instructs the bots what, when, how, whom to accomplish attack. To elude detection botmaster can alternatively put many proxy machine called stepping stone between them and Command & control centre.

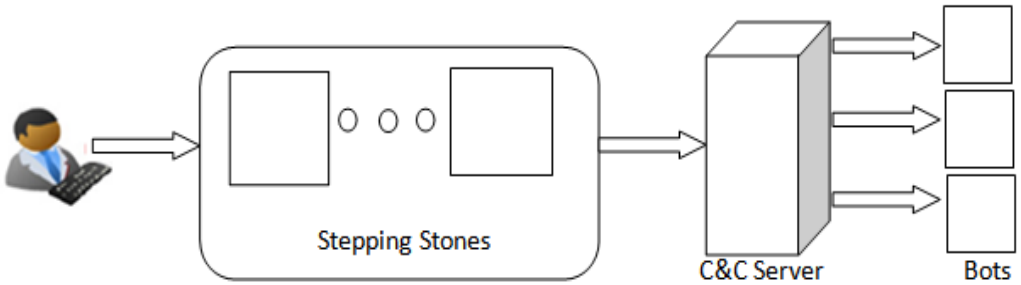

Figure 1. Structure of a Typical Botnet

The Botnet is having multiple architecture and different bots associated to different botnet communicates with botmaster and others bots based upon the type of architectures. The bots used various approach like IRC or HTTP etc in which IRC were very common. Mainly three kind of architecture followed by the bot master to communicate with the bots Web-Based Model[6], Agent-Handler model and IRC Model.

2. Related Work

The basic motive behind the detection is to identify the malware present in the mobile application and if detected can be blocked , quarantined or removed. various proposal of detection procedure associated with Smartphone has been proposed by [7]-[12].However these scholar concentrated on mobile malware detection and mobile botnet basic detection approach and the commonly used approaches are static analysis and dynamic analysis.

Static Analysis

Static analysis requires different binary forensic techniques containing decryption, decompilation pattern matching and static system call anaysis, . Static analysis can be exactly implemented either on application source code or binary representation and can use reverse engineering method to extricate some characteristic or features which may invoked from source code. Not only to recognize spiteful payload but also profile and weigh malware threat[13] extracted features is applied. There are various techniques used for static analysis for example File fingerprinting, Extraction of hardcoded string, AV Scanning, packers detection, etc. Static analysis is easy and systematic in giving quick detection but for the known malware and fails to provide detection for the unrevealed or complex malware and also consumes lot of time making it almost impossible to identify the new malicious polymorphic code without manual intervention.

Dynamic Analysis

Dynamic analysis performed and monitored the malicious application during the run time through tools. The malicious application movement can be examined through system call, logged Behaviour sequence, Dynamic Tainting, Control Flow, monitoring file changes ,network activity and Data Flow. So it is simple to view the real behaviour of the program and another benefit is that because it can be automated which help to trigger analysis at larger scale.

Related Studies on Mobile Malware Detection

The First effort to recognize and examine the malware on the mobile phones introduced by existing PC Security Solution but this was not the reasonable solution

Schmidt is one the person who suggested mobile malware detection for Android Smartphone[14] . This proposed algorithm derive function calls from binaries of application and for detecting unrevealed malware a clustering mechanism called Centroid is used .Which is achieved by implementing static analysis of Executable and Linking Format(ELF) objects files by utilizing command readelf in Android. The function calls and modified files which maintain those file data are compared with malwares executable for arrange them with DTL(Decision Tree Learner), Rule Inducer (RI) and), Nearest Neighbour (NN) algorithm. The author challenged that this algorithm shows up to 96% detection perfection with 10 % false positives. The major disadvantage of this technique is that it is implemented in small collection of samples and manually coded any nowhere available in real market.

Static analysis used by [15] and author suggest Android malware detection mechanism called DroidMat. It reveals malware through and traces of API calls and manifest file. They Challenged that this tool is much efficient to identify more malware then other detection tool, the AndroGuard

but only one sample of android malware can't estimate and study pattern of newly detected malware. Besides this there are some pattern of malware (BaseBridge and DroidKungFu) which implemented revised scientific procedure which is not identified by DroidMat [16].

In the year 2010, [17] et al. proposed a mobile malware detection technique which examine different attributes receiving from the Smartphone during the application execution. Further they used machine learning anomaly detectors to categorize the sample or data which is collected as normal for obliging or uncommon for spiteful. The attributes is considered on the basis of number of packet sent through wifi cpu consumption, pressing keyboard or touch screen, number of running process and application start-up. To prove proposed model they picked attributes using 3 selection technique , Chi-Square Information Gain, and Fisher Score. There are two disadvantage of this technique , system is not using any real time malware sample use of application that imitate user interaction called ADB monkey(means proxy user)

In [11] proposed a technique which dynamically analyze the behavior of Mobile(Android) Applications. For getting the traces of application behavior like system call they applied CrowDroid which is a crowd-sourcing system. In the runtime CrowDroid gathered the system calls which is used by the set of user. To categorize the data in to dual group named benign group and the malicious group they chosen K-means clustering technique which can be applied to detect the end user running the infected repackaged application. The proposed algorithm required a set of user to run the actual application and the identical malicious application However the drawback of this algorithm is that it is tested using self implemented set of malware samples and applied small scale of malicious dataset but the result shows cent percentage of perfection.

[10] proposed AAsandbox which is capable of performing both static and dynamic analysis of application. AAsandbox consists of apk,static and dynamic analysis method

and resulting dataset for further analysis. During application execution in Android Emulator , AAsandbox counts the number of all system call to detect the malicious behaviour but the results getting during this is very different and thus less detection rate[18]

[8] proposed a different static analysis which examine the applications for getting malicious design Kirin. They defined different threatening approved mixture as protocol to stop the installation of infected software. Although Kirin is more about vulnerability evaluation rather than mobile malware

All the above works have its own potential and drawbacks that can be improved in future. It is also observed that mostly all the work focuses on mobile malware detection but the most hazardous and threatening is mobile botnet[1],[19].A research[20] shows that out of 1260 mobile malware samples 93% shows mobile botnet behavior.

Human Immunology System (HIS) which helps human to adopt in the difficult or changing atmosphere now a days many research is going on in this basis i.e to design a computer based Artificial Immune System (AIS).AIS is applied to block or neutralize the virus or infected applications. Somayaji, et. al.,[20] given different architecture of Artificial Immune System for security.

3. Problem Scenario

This section explain the problem scenario how the hacker hacks the bank customer mobile and their computer.

1. Unknowingly when customer respond to the phishing email, DDos or click fraud which tempts the user to click on the spurious url. The Trojan is downloaded and install on the customer desktop after clicking the link and Trojan is waiting for the user to login into his/her account.
2. .As the Customer login in to e bank account Eurograbber Trojan virus obstruct the session and insert a script into the customer banking page this script notify the customer regarding "security update" and provide instruction to proceed further

Instruction may be in below format:-

To stay protected you need to install the software to update your mobile:-
Please choose which OS you are using:

- BlackBerry
- Android
- Symbian
- IOS
- Other

Please enter your mobile number

Below code used to inject above message on customer mobile

```
jQuery(document).ready(function(){
INJ.phones=function(){    -->Mobile phone and OS details
this.vendor=io.observableArray();
this.selectedVendor=io.observable();
this.model=io.observable({});
this.selectedModel=io.observable();
this.getName=io.computed(function(){
 if(this.selectedVendor()&&this.selectedModel()){
 var lst;
 for(var j in this.selectedModel()){lst=j};
return this.selectedVendor()+'_'+this.selectedModel()[i].model;
```

3. The Trojan then provide the customer mobile details to the dropzone which is stored and used on next attack.
4. Now attacker got customer mobile details which prompt the Eurograbber to facilitate an message on customer mobile via mobile network in their local language. The SMS instructs the user to update the security by clicking the attached URL. After completion a file has been downloaded on customer mobile with exact mobile version of the Eurograbber Trojan.

Below code has been injected for this requested to click:-

```
jQuery.ajax({
url:'https://xxxxxxxx-c.com/sms.php',  -->sms sending system location
data:{
        num:phone,  -->customer mobile number
    lang: 'nl,  -->application language.
    type:tGo.data('mobile_type')
```

5. Concurrently Customer also receive sms on mobile which instructs them to follow the steps mentioned in the message to update the software. On completion customer have to enter the verification code which is send in their native language which confirms that the mobile updation activity completed. Now the User is now administered by Eurograbber attacker. The Customer got a message by the attacker saying that your software has been successfully updated and no further security needy in your mobile. The software is installed correctly and at the same moment Eurograbber contaminate both mobile and desktop of the customer and can seize all the transaction without customer awareness even.
6. Now whenever customer login to their bank account the attacker begin Eurograbber's desktop Trojan to initiates its own transaction to dummy account hold by attackers. When illegal online banking is submitted the bank trigger a TAN (Transaction Authorization Number) in mobile through short message service but now here Eurograbber's mobile Trojan play their role and obstruct the message having TAN Number conceal it from the customer and redirects to relay phone number and further to the drop zone where it is kept in the C&C(command and control) database with additional customer information, to make the process complicated the message does not stored directly in dropzone.
7. Now the TAN number is taken from the dropzone by the desktop Trojan and ten sends to the bank to finish the illegal transaction. The victimized customer bank account lose their money to dummy hacker account without customer awareness.

This is a continuous process which will happen with customer information whenever they will do online transaction.

4. Proposed Solution

During the time of registration the customer has to provide the their voice sample in the bank voice biometric authentication system database which will only be executed if customer's account is on the radar of Eurograbber attacker. If any of the above three mentioned factors fails the transaction seems to be under the radar and it has to go through the Voice biometric authentication process. Customer login into their bank account enter userid and password click to perform monetary transaction then immediately system will check the

"Location of accessing account", "Network analysis parameter" and "Time between operations within one session" if any one fails the transaction is suspended and user has to go through the voice biometric authentication if voice matches with the stored sample in the bank database then transaction performed else the transaction will be cancelled.

Location of accessing account:

If transaction is carried out from high unsecured zone or high risk country then transaction may be blocked, Also based on the previous transaction history location, customer online transaction may be cancelled if crossed certain geographical distance.

Network analysis parameter:

The current transaction may be cancelled if IP address matches with the list of blacklisted IP addresses or if carried out with any anonymous IP address.

Also if Operational activity from any one IP address is more or if its frequency is very high or if from same IP address is used to access several customer account then that IP address may be put under sceptical category and the transaction may be cancelled.

Time between operations within one session:

The average time should be carried out based on the user profile history and if it takes less duration of time then that session may be hacked so the transaction may be cancelled immediately.

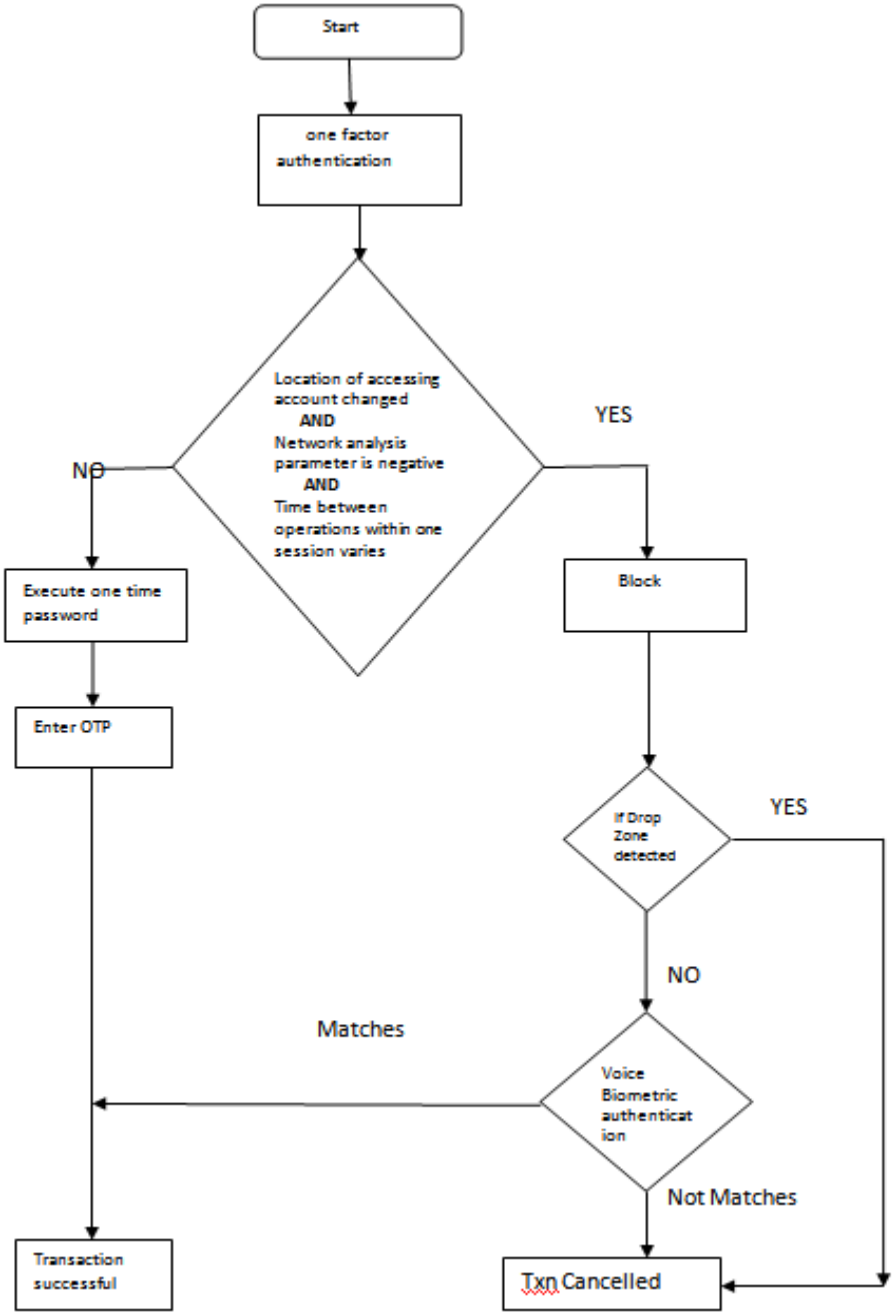

Figure 2. Proposed Model for Protecting Eurograbber Attack

5. Conclusion and Future Work

Eurograbber is becoming a major challenges for the sercurity expert.This Model will help to strenthen the online banking security. The information such as the user credentiaal, passwords,mobile number,application installation status,mobile operationg system etc are stored in Drop Zone. The major work we need to perform is to identify the dropzone which is managed by the Eurograbber attacker and immediately need to canel the transaction immediately if dropzone is detected. Also need to write an appropriate algorithm which can do the network analysis parameter checking effectively.The whole installation process of the infected software is only installed when a bad url is sent via SMS we need to find out the algorithm and technique which can stop recieving the

mesaage on mobile which may stop the Sophisticated Eurograbber attack in the initial level itself.The bank has to develope the algorithm which can start the biometric voice registration process when the customer register with the bank and aslo have to maintained the high secured database for storing the voice biometric authentication samples.

References

[1] M. Eslahi, R. Salleh, and N. B. Anuar, "Bots and botnets: An overview of characteristics, detection and challenges," 2012 IEEE Int. Conf. Control Syst. Comput. Eng., pp. 349–354, Nov. 2012.
[2] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," IEEE Commun. Surv. Tutorials, vol. 15, no. 1, pp. 446–471, Jan. 2012.
[3] H. Pieterse and M. S. Olivier, "Android botnets on the rise: Trends and characteristics," in 2012 Information Security for South Africa, 2012, pp. 1–5.
[4] https://en.wikipedia.org/wiki/EMarketer
[5] Alomari, E.,., Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. arXiv preprint arXiv:1208.0403, 2012.
[6] Barthakur, P., M. Dahal, and M.K. Ghose, An Efficient Machine Learning Based Classification Scheme for Detecting Distributed Command & Control Traffic of P2P Botnets. International Journal of Modern Education and Computer Science (IJMECS), 2013. 5(10): p. 9.
[7] A. Schmidt, R. Bye, H. Schmidt, J. Clausen, O. Kiraz, K. Yuksel, S. Camtepe, and S. Albayrak, "Static analysis of executables for collaborative malware detection on android," IEEE Int. Conf. Commun. 2009, pp. 0–4, 2009.
[8] W. Enck, M. Ongtang, and P. McDaniel, "On lightweight mobile phone application certification," in Proceedings of the 16th ACM conference onComputer and communications security - CCS '09, 2009, p. 235.
[9] A. Shabtai, Y. Fledel, and Y. Elovici, "Automated Static Code Analysis for Classifying Android Applications Using Machine Learning," 2010 Int. Conf. Comput. Intell. Secur., pp. 329–333, Dec. 2010.
[10] T. Bläsing, L. Batyuk, A. Schmidt, S. A. Camtepe, and S. Albayrak, "An Android Application Sandbox system for suspicious software detection," in 2010 5th International Conference on Malicious and Unwanted Software, 2010, pp. 55–62.
[11] I. Burguera and U. Zurutuza, "Crowdroid : Behavior- Based Malware Detection System for Android," Proc. 1st ACM Work. Secur. Priv. smartphones Mob. devices (SPSM '11), 2011.
[12] M. Grace, Y. Zhou, Q. Zhang, S. Zou, and X. Jiang,"Riskranker: scalable and accurate zero-day android malware detection," Proc. 10th Int. Conf. Mob. Syst. Appl. Serv. (MobiSys 2012), pp. 281–293, 2012.
[13] S. Y. Yerima, S. Sezer, G. McWilliams, and I. Muttik, "A New Android Malware Detection Approach Using Bayesian Classification," 2013 IEEE 27th Int. Conf. Adv. Inf. Netw. Appl., pp. 121–128, Mar. 2013.
[14] D. Damopoulos, G. Kambourakis, S. Gritzalis, and S. O. Park, "Exposing mobile malware from the inside (or what is your mobile app really doing?)," Peer-to-Peer Netw. Appl., Dec. 2012
[15] D.-J. Wu, C.-H. Mao, T.-E. Wei, H.-M. Lee, and K.-P.Wu, "DroidMat: Android Malware Detection through Manifest and API Calls Tracing," 2012 Seventh Asia Jt. Conf. Inf. Secur., pp. 62–69, Aug. 2012
[16] L. K. Yan, "DroidScope : Seamlessly Reconstructing the OS and Dalvik Semantic Views for Dynamic Android Malware Analysis."
[17] A. Shabtai and Y. Elovici, "Applying behavioral detection on android-based devices," Third Int. ICST Conf. Mob. Wirel. MiddleWARE, Oper. Syst. Appl., pp. 235–249, 2010.
[18] C. Mulliner. Exploiting symbian: Symbian exploitation and shellcode development. http://mulliner.org/symbian/feed/CollinMulliner_Exploiting_ Symbian_BlackHat_Japan_2008.pdf, 2008. Talk on BlackHat Japan 2008, visited 15.6.2009.
[19] Y. Zeng, K. Shin, and X. Hu, "Design of SMS
[20] commanded-and-controlled and P2P-structured mobile botnets," WISEC '12 Proc. fifth ACM Conf. Secur. Priv. Wirel. Mob. Networks, no. February, 2012
[21] A. Somayaji, S. Hofmeyr, and S. Forrest, "Principles of a computer immune system," in Proceedings of the 1997 workshop on New security paradigms - NSPW '97, 1997, pp. 75–82

