IOSR Journal of Computer Engineering (IOSR-JCE)

e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 6, Ver. I (Nov – Dec. 2015), PP 113-118

www.iosrjournals.org

"Design and Detection of Mobile Botnet Attacks"

Aishwarya A. Bhandari[1],Jyoti D. Bhalchim[2], Suman P. Bansode[3], Anuja Lambate [4],Prof. Sonali Tidke[5]

[1,2,3,4]*Department of Computer Engineering, Savitribai Phule Pune University Pune, Maharashtra, India*
[1,2,3,4]*Pimpri Chinchwad College of Engineering Sector No.26, Pradhikaran, Nigdi, Pune, India*

***Abstract**: A mobile botnet is a type of bot that runs automatically when installed on a mobile phone, which does not have any anti-malware. The botnet gains complete access over our mobile device. The common propagation medium for smartphone based botnet attacks are SMS, Bluetooth and Wi-Fi. In our project, we will demonstrate a SMS-cum-Wi-Fi based mobile botnet using a centralized C&C server. The botmaster initiates commands to C&C server and the C&C propagates to infected smartphones i.e. bots. We will try to develop a network which cannot be detected easily and propagates fast. The target of the propagation will be Android Operating System. For detection, an application is created to detect whether smartphone is working as bot or not. In this, we guide user about possible botnet attacks.*

***Keywords**: Botnet , Botmaster , Smartphone , C&C , Bot , Attacks , Malware , Botnet Detection.*

I. Introduction

Smartphones are mini laptops for user. We use them not only for calling but also smartphones are used for banking, shopping, mailing, web surfing, etc. Most of the smartphones user store their important as well as personal information on the smartphone. A drastic increase in downloading and sharing of third-party applications and user-generated content makes smartphones vulnerable to various types of malware.

Smartphone-basedbanking services have also become popular without protection features comparable to those on PCs, enticing cyber crimes. There are already a number of reports on malicious applications in the Android Market. Although the Android platform requires that applications should be certified before their installation, its control policy is rather loose allowing developers to sign their own applications so that attackers can easily get their malware into the Android Market. The iPhone's application store controls its content more tightly, but it fails to contain jailbroken iPhones which can install any application and even run processes in the back- ground. As smartphones are increasingly used to handle more private information with more computing power and capabilities, but without adequate security and privacy protection, attacks targeting mobile devices are becoming more sophisticated. Since the appearance of the first, proof-of-concept mobile worm, Cabir, in 2004, we have witnessed significant evolution of mobile malware. The early malware performed tasks, such as infecting files, replacing system applications and sending out SMS or MMS messages.One malicious program is usually capable of only one or two functions. Although the number of mobile malware families and their variants has been growing steadily in recent years, their functionalities have remained simple until recently first Android bot, Gemini, was discovered in China in December 2010. It was a trojanized game application. Gemini steals infected device's International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), GPS coordinates, contact list, SMS details etc and used to forward it to the botmaster.

We proposed the SMS and WiFi based heterogeneous mobile botnet model. The C&C channel is SMS based heterogeneous network. That is, all C&C commands are transferred via SMS messages since SMS is available to almost all mobile phones and we use Wifi to propogate bot faster.

Objects Involved:

1) Botmaster :

Bot master controls all the nodes of the mobile botnet. The bot master has direct contact with Bot Servers.

2) Bot :

Bot is the leaf node of our model. It receives commands from region bot server, and executes the commands.

3) C&C Server :

A command and control server (C&C server) is the centralized computer that issues commands to a botnet (zombie army) and reports back from the infected computers.

II. History Of Mobile Botnet

The first generation of computer-based botnets, were established over IRCs and then evolved to P2P and HTTP mechanisms. While it is difficult to implement a wide variety of C&C models for mobile based botnets due to the lack of public IP addresses, availability of variety of operating systems, different types of connectivity mediums and the cost of communication.

A Symantec-commissioned Strategy One report found that 65 percent of computer users have spent 28 hours and $300 dealing with cybercrime; McAfee estimated a $1 trillion global cost. A single botnet ring took $100 million before the FBI managed to stop it. The UK government estimates that each year the country loses 27 billion to cybercrime, which extrapolated to the US population and converted to dollars would be approximately $210 billion. The UK's response will be 650 million for cyber security. A few years ago, Consumer Reports gave a relatively low number for US cybercrime loss-$7 billion over two years, whereas The Washington Post suggested a cost of $105 billion per year. Another large study estimated that cyber fraud and the like cost between 0.2 percent and 0.4 percent of global GDP, or approximately $100 to $200 billion.[1]

The person in charge for the botnet attack is known as Botmaster. The Botmaster sends a SMS that contains malicious data in it, to the C&C (Command and Control) servers. The C&C servers itself is a victim which is unaware of the botnet attacks. The C&C servers automatically forward propagates the same message to their contacts, i.e. victims. The C&C server forwards as well as reports the contact details to the botmaster. The victims or infected systems forward the same message and further create more bots. But these contacts report all the details at C&C server and then to the Botmaster.

III. Challenging Issues

· ***Generally, the hackers have to overcome the following challenges to design an effective SMS-based mobile botnet:***

The proposed botnet should have an efficient C&C architecture, in which a command issued by the botmaster can reach most of the bots in a short time. What's more, for security reason each bot should only send a small number of SMS messages in this process.

Because all the SMS messages are under the monitoring of the telecom operators, we need special measures to disguise the botnet messages as the legal ones to evade being filtered out.

Once a botnet is constructed, we need special mechanisms to maintain it. This mainly involves two issues: Firstly, the botmaster usually wants to master the runtime statuses of their controlled bots. Thereby, besides a command propagation channel, we need another reporting channel from the bots to the botmaster. Secondly, the botmaster has the requirement to update the malware distributed on the bots regularly. The sizes of these updates usually greatly exceed the maximum payload of a single SMS message, so we need an extra updating mechanism.[2]

IV. Motivation

Mobile botnet attacks on cellular networks and devices have recently grown in number and sophistication. With the rapidly-growing popularity of smartphones, such as the iPhone and Android-based phones, there has been a drastic increase in downloading and sharing of third-party applications and user-generated content, making smartphones vulnerable to various types of malware. Security wise and financial charge wise, lots of research is required in this field. So the main aim of the proposed research work is to detect mobile botnet attacks by guiding user about possible attack. This research work is mainly focused on safeguarding mobile phones from ever growing and varying
technologies of botnet attack.[1]

V. Proposed Methodology

PC based botnet attacks are now known to the world and like other malware and spam activities, anti malwares are available to monitor and detect them. But considering the scenario of mobile based botnet attacks, it is still very new and unknown to the world of cyber users. Smart phone users still blindly trust on applications and default settings of smart devices and are using them without knowledge of risk associated with it. Though mobile botnet is a pretty new concept for users, it is not much known to cyber researchers too. Research work on mobile botnet is still in the initial stages of detecting and stopping them from propagation. Though researchers are developing various ways for detecting botnet, not a guaranteed technique is provided to stop propagation.[1]

"Design and Detection of Mobile Botnet Attacks"

Objective of our project :

1) Design :

Creating a network of bots and communicating together which report and receive orders from a C&C (Command and Control) server, allowing the person in charge (i.e. Botmaster) to leverage the computing power of all the bots in the botnet as required.

2) *Detection :*

- Creating an application to detect if smartphone is working as active bot or not.
- Guiding user about possible botnet attack.

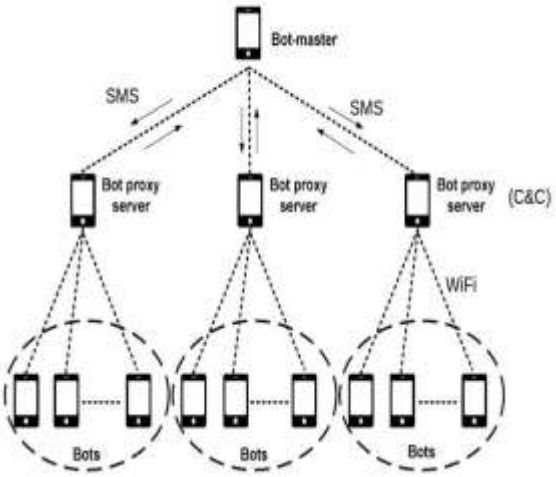

Fig : Proposed Botnet Architecture

Centralized architecture is easy to implement and detect while P2P is difficult to detect and implement too. In this research we are using Hybrid architecture for developing botnet[3]. Above figure shows architecture of proposed botnet. Here, botmaster can be either a smart device or a desktop PC which will work in isolation to avoid detection. Botmaster maintains a list of C & C servers and gives commands to propagate to bots. After a particular duration, Botmaster can remove C & C server from its list of servers to avoid detection. Infected bots can also work as C & C server if required.

We proposed SMS and WiFi based heterogeneous mobile botnet model. The C&C channel is SMS based heterogeneous network. That is, all C&C commands are transferred via SMS messages since SMS is available to almost mobile phones and we use WiFi to propagate bot faster.

Detection of Bot :

Detection of Smartphone based botnet attack is still area of research. Proposed system will help to detect such attacks to prevent our smartphones from exploitation.

Following are the few symptoms that would help the application to detect whether the system is a bot or not :

1) IRC traffic (botnets and bot masters use IRC for communications)
2) Connection attempts with known C&C servers.
3) High outgoing SMTP traffic (as a result of sending spam).
4) Unexpected popups (as a result of clickfraud activity).
5) Slow computing/high CPU usage.
6) Outbound messages (email, social media, instant messages, etc) that weren't sent by the user.

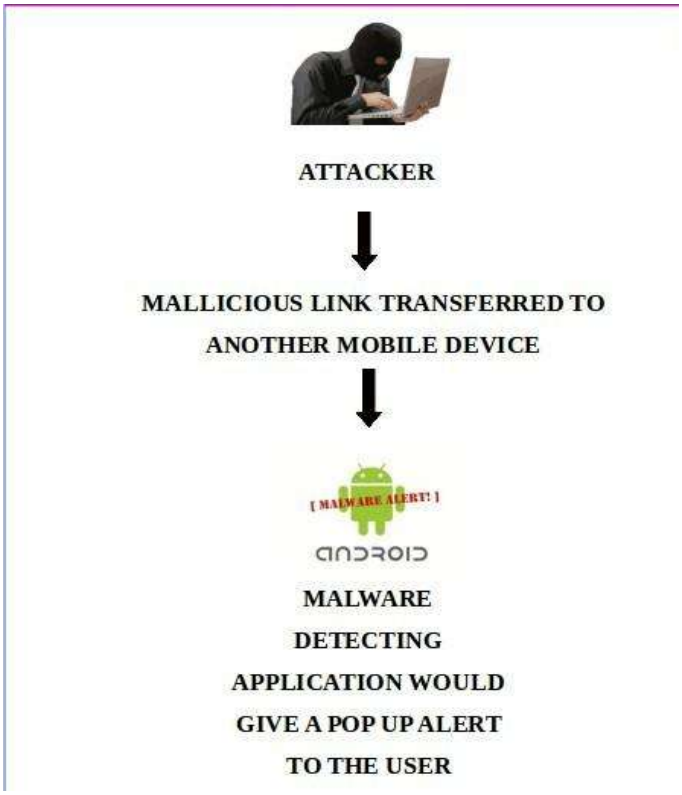

Fig : Botnet Detection Flow

We are going to design an application which detects whether the system is a bot or not. The app would also alert the user, which applications are not trusted, if the user clicks OK on the pop message, those untrusted applications would be directly uninstalled. Also a list of trusted and untrusted app would be maintained by the user.

Fig. : Working of Botnet Detection App

VI. Algorithmic Steps

Consider following steps for designing and detecting a mobile botnet :

Steps for designing botnet :

1) Botmatser will send some eye catching web link to few (200-300) users through sms.
2) Once user clicks on the link, malware get installed and it will upload users contact list on server. Infected smartphone work as bots C&C. Botmaster will maintain list of bot C&C, Name, its IMEI,IMSI and MAC

addresses.

3) This uploading will happen without users intervention.
4) Botmaster can found out password call number, credit like words from contact details of users.
5) Botmaster can send multiple messages to infected bots or can ask bots to send same messages to their contact details through social network site.
6) Botmaster will also maintain list of bots infected through which C&C, so that same should not resend again.

Steps for Detecting Botnet :

1) Find the list of all trusted apps & their read permission.
2) Maintain list of trusted app/third party app & read permissions on users mobile.
3) If an app requires permission which is irrelevant, ask user to modify permission.
4) If app is not used from long time, inform user to delete application.
5) Inform users about third party apps not installed through play store.
6) Guide user if app requires extra permission than read & maintain list of apps that are not useful.

Following figure shows Flowchart for Detecting a Mobile Botnet attack :

most serious threat to it. Hence, it is very important to detect botnet attack and find a solution for it. In our future work, we track down botmaster as early as possible and generalize guidelines for all type of smartphones. Once the bot has been detected on a host, we determine what kind of actions should be taken to mitigate the affect of the bot and how to respond to this threat. We plan to examine this area in our future work.

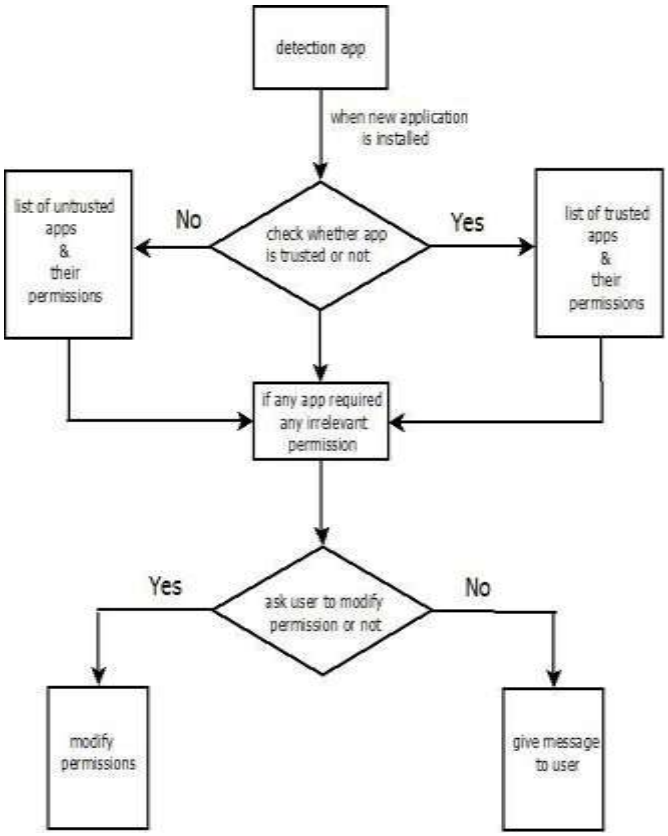

Fig: Flowchart for detecting botnet

VII. Usefulness Of Proposed System

· It is useful for providing security that affect smartphones.

· Notify end users about remotely identified infections through their Internet Service Providers is useful and effective approach.

VIII. Conclusion And Future Work

Botnets pose a significant and growing threat against cyber security. It provides key platform for many cyber crimes. As network security has become integral part of our life, botnets have become most serious threat to it. Hence, it is very important to detect botnet attack and find a solution for it.In our future work, we track down botmaster as early as possible and generalize guidelines for all type of smartphones. Once the bot has been detected on a host, we determine what kind of actions should be taken to mitigate the affect of the bot and how to respond to this threat. We plan to examine this area in our future work.

IX. Acknowledgment

We express our sincere thanks to our Project Guide Prof. **Mrs. Sonali Tidke** for her encouragement and support throughout our seminar, especially for the useful suggestions given during the course of project and having laid down the foundation for the success of this work. We would also like to thank our Project Co-coordinator **Mrs. Sonali Tidke** for her assistance, genuine support and guidance from early stages of the seminar. We would like to thank **Prof Dr. K. Rajeswari**, Head of Computer Engineering Department for her unwavering support during the entire course of this project work. We also thank all the staff members of our department and technicians for their help in making our project work successful. We also thank all the web communities for enriching us with their immense knowledge.

References

[1] Prof. Sonali Tidke,Dr. Pravin Karde,International Journal of Advanced Research in Computer Science and Software Engineering,Volume 5, Issue 4, April 2015,ISSN: 2277 128X.

[2] Jingyu Hua ⋆ and Kouichi Sakurai,A SMS-Based Mobile Botnet Using Flooding Algorithm,Department of Informatics, Kyushu University, {huajingyu, sakurai}@itslab.csce.kyushu-u.ac.jp.

[3] Mrs. Sonali Tidke,International Journal of Advanced Research in Computer Science and Software Engineering,Volume 4, Issue 2, February 2014,ISSN: 2277 128X.

[4] Guining Geng, Guoai Xu, Miao Zhang, Yixian Yang ,Guang Yang,An improved SMS based heterogeneous mobile botnet model,Proceeding of the IEEE International Conference on Information and Automation Shenzhen, China June 2011

[5] Meisam Eslahi,Rosli Salleh,Nor Badrul Anuar,MoBots: A New Generation of Botnets on Mobile Devices and Networks, 2012 International Symposium on Computer Applications and Industrial Electronics (ISCAIE 2012), December 3-4, 2012, Kota Kinabalu Malaysia.

[6] David Dagon, Guofei Gu, Cliff Zou, Julian Grizzard, Sanjeev Dwivedi, "A Taxonomy of Botnets," University of Central Florida.

[7] Mohammad Reza Faghani and Uyen Trang Nguyen,SOCELLBOT: A NEW BOTNET DESIGN TO INFECT SMARTPHONES VIA ONLINE SOCIAL NETWORKING.

[8] P.Traynor, M.Lin, M.Ongtang, V.Rao, T.Jaeger, P.McDaniel, and T.L.Porta, "On Cellular botnets: Measuring the impact of malicious devices on a cellular network core," in Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS'09).