Design Methodology of Botnet Attack for Smartphone

Prof. Sonali Tidke and Dr. Pravin Karde

ABSTRACT : *Smartphones are mini laptops for its users. Besides calling, smartphones are used for banking, shopping, mailing, web surfing, socializing etc. Most of the smartphone users are storing their important, personal and sensitive information on their device without providing sufficient security and are unaware of the risk involved in it. This paper provides a closer look on how smartphone Botnet can do if not secured properly.*

Keywords *- C & C, IMEI, IMSI, OSM, HttP2P*

I. INTRODUCTION

Botnet is a large network of compromised computers. A bot can form a network of compromised computers that are controlled by botmaster or herder [1] and uses a command and control (C & C) server. Compromised computers, also called as zombies, are turned in to a bot. This occurs when a user downloads or opens a malicious software application. The word Botnet is combination of two words robot and network, so can be called as network of robots. Though PC based Botnet is now well known to cyber community, smart device based Botnet is new and such attacks are growing in cyber world. PC based BOTNETs are active from almost two decades in cyber world.

First smart phone based Botnet, Cabir, appeared in 2004 while 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 [2].

II. PURPOSE OF MOBILE BOTNET ATTACK

Development of malwares is not having any specific reason but following can be few reasons why cyber criminals are taking interest in developing mobile botnet attacks:

a) Information Leakage: One of the main targets of the mobile botnet is to retrieve sensitive information from the victims. The mobile bot can quickly scan the host node for significant corporate or financial information, such as usernames and passwords, address list and text messages.

b) DoS Attack: Because most of the functionality of cellular network rely on the availability and proper functioning of HLRs (Home Location Register), so the DoS attack could block the legitimated users of a local cellular network from sending or receiving text messages and calls [3].

c) Charge loss: There exists some service which the smart phones can give money to charity organizations. If the mart phone called or sent a text message to the specific service number, then the subscriber will pays a preset amount of money. The bot master can also creates its own service number and programs all the bots to call or sent a text message to the specific service number [3].

Other genera reasons includes:

1. Frequent downloading and sharing of third party applications and contents generated by end user
2. Increasing processing power and memory capacity of memory
3. Storage of personal and confidential, sensitive data
4. Availability of various communication mediums
5. Lack of security and unawareness of end user about cyber risk.

III. DESIGN AND WORKING OF BOTNET ON SMARTPHONE

Considering the unique features of mobile devices, mobile Botnet can take its advantage to be more stealthy and resilient from detection. Mobile devices can communicate via multiple vectors including SMS/MMS, Bluetooth, NFC besides conventional IP network. As mobile devices move around frequently, it is difficult to find exact points that can observe all devices' activities. Also, current smart phone users tend to download and share third party applications without any security and opening doors for cyber attacks.

Each Botnet developer designs its Botnet in such a way that it should not get detected easily. Botnet can be designed using different methods and can be propagated using various propagation medium. Similar to PC based Botnet, mobile Botnet have components like:

1) Botmaster: Sometimes also referred as backend server or Botnet controller. Botmaster is a person who operates network of bots. Botmaster is responsible for maintaining network, keeping bots online, fixing errors and forwarding new commands to C & C server. Botmaster often hide identity behind proxies, Tor network to disguise its IP address from detection by investigators or law enforcement. The bots are configured to authenticate the command and control station via password and/or keys to allow remote control. In some cases a Botnet is shared, and multiple botmasters operate it together. It is also commonplace for hacking the Botnet credentials or otherwise taking control of another botmaster's Botnet [4].
2) Command and Control Server: This is a centralized computer which issues commands to zombies on behalf of botmaster and receives reports back from them. Depending on the infection and propagation methodologies Botnet can have multiple C & C servers. The term originated from the military concept of a commanding officer directing control to his/her forces to accomplish a goal [5].
3) Bots: A bot (short for "robot") is a program that operates as an agent for a user or another program or simulates a human activity [6].

This paper presents proof-of-concept of Botnet design on smart phones. This requires a vector for spreading bot code to mobile phones, propagation medium to spread commands and topology required to manage Botnet.

- Propagating malicious code on smart phones can be done via user involvement or by exploiting vulnerabilities of smart phone OS and its applications. Smartphones have frequent access to Internet which makes them vulnerable for cyber attacks. Thus, using spam mails or MMS with malware code attached or SMS with a website link having malicious code available on server, can easily find a way into smartphone users inbox. Without enough caution, a mobile phone user executes such attachment or click on links in mails/messages. This way malicious code can reach a large number of phones in minimum time span. The same way Bluetooth can be used for propagating commands. An infected smartphone can move around, try to pair with other smartphones and infect them by sending malicious files. For example, HTC's Bluetooth vulnerability allows an attacker to gain access to all files on a phone by connecting it via Bluetooth. In [7], author has discovered a way of directly manipulating SMS messages on different mobile OS without communicating directly thru mobile network provider.
- Exploiting vulnerabilities of OS is common in PC world but most of the mobile operating systems are closed source. As the market of Android (open source OS) is increasing day by day, new attacks are developed and launched to exploit weaknesses of open source OS.
- Use of SMS by C & C server is a very common method. C & C servers communicates and propagate commands to bots via SMS. Use of SMS provides various advantages for spreading attacks like when a phone is turned on, SMS becomes active. Likewise, SMS can accommodate offline bots easily. Also malicious contents can in the C & C communication can be hidden in SMS easily. Few examples of use of SMS over Android OS are presented here. A random invitation received via SMS to download free version of popular Android games like The Need for Speed or Angry Birds Star Wars can lure smartphone user. Once user downloads this malicious application and install it on Android smartphone, user may loading a malicious software which can convert the smarphone in to active bot. Once converted as bot, the phone will be used to silently send out thousands of spam SMS messages without user's permission to lists of victim phone numbers that the malware automatically downloads from a command and control server.

In [8], it is mentioned that the Trojan apps were downloaded from sites on a server in Hong Kong offering free games. They claimed to be copies of popular games including the ones mentioned above. Along with free game messages, spammers also started floating free gift card scam messages.

Following is a fairly common sort of SMS spam:

> “*You have just won a $1000 Target Gift Card but only the 1st 777 people that enter code 777 at http://[redacted].com can claim it!*”

There are of course not any free gift cards; this is just a trick to collect users’ personal information for related spam programs and sometimes identity theft purpose [9].

- Besides Bluetooth and SMS, newly used medium for propagating attacks is OSM i.e. Online Social Medium. Today’s users don’t only access or surf internet on smartphone. They use smartphone for accessing/storing personal details, banking information, health details etc. Similarly users use smartphone to communicate with friends/society using various social apps like facebook, orkut, twitter, hike, whatsapp etc.

IV. Botnet Architecture and Detection Techniques

Botnet uses various types of architectures to control its network and to avoid detection. Botnet architecture can be Centralized architecture, hybrid architecture, P2P (Peer to Peer) architecture, combination of HTTP (Hyper Text Transfer Protocol) and P2P i.e. HttpP2P.

1. Centralized Botnet Architecture: This type of architecture is easy to manage and control. All infected bots can be monitored and controlled thru a single point. This is the most easiest to develop and detect architecture. AgoBot, SDBot, Zotob, SpyBot, GTBot are few examples of centralized C & C architecture [10].
2. P2P architecture: To overcome drawbacks of centralized architecture, cyber criminals have focused on P2P architecture. In this type of architecture, botmaster sends commands to multiple C & C servers. These servers acts as peers and propagates them further to create new bots. In this peers maintain their own list of commands and infected bots. This architecture is difficult to ardetect. Phatbot and Peacomm bots are examples of P2P architecture Botnet [11].
3. Hybrid P2P architecture: This is similar to P2P architecture where botmaster creates several C & C servers. Each C & C server spreads commands to network along with communicating with other peer servers. If a peer server fails, its work will be handled by other peers and will work as distributed network of bot servers. This kind of Botnet architecture is tough to manage and at the same time it makes detection of botmaster much difficult. In [11], Ping Wang et. al. has designed and proposed a hybrid P2P attack architecture which is difficult to detect and observe.
4. HttP2P architecture: P2P architecture suffers from threat of Sybil attacks [12]. Combination of Http and P2P makes detection of Botnet much harder. In this type of architecture, botmaster cipher the message and continuously search for bot which can work as soldier of bot army. Once found, botmaster delivers message to soldier bot/peer server. While peer server does not contact dynamically to botmaster or other peer servers, instead it just waits for a call from botmaster.

Cybercriminals are finding newer methods regularly for developing Botnet to avoid detection. As C&C traffic appears as legitimate traffic, it is tough to identify bot attack to save networks. Researchers are providing different algorithms, methods, techniques to make Botnet attack detection in early stages. Few commonly used techniques of Botnet detection are signature-based detection, honeypots, analyzing the DNS traffic and behavioral analysis.

1. Signature Based Detection: Signature refers to the detection of Botnet from known pattern and characteristics. By analyzing and comparing available patterns, malicious activities can be distinguished from normal ones. This method simply compares available patterns of known bots. This method is useful for detecting known bots but not for the new ones [12,13]. This detection technique is now not used for Botnet detection as it cannot identify new patterns or characteristics.
2. Honeypots: This is a type of trap used to collect information about bots’ and analyze their working and activities. It helps in finding more information about botmaster. Honeypots can be low interaction honeypot or high interaction honeypots. Low interaction honeypots provide limited communication between server and botmaster which is meant for collecting basic information of botmaster activities. To collect more details of botmaster activities, organizations use high interaction honeypots which provides access to real systems and services. This provides botmaster more control over the network. Though this approach is helpful in collecting detailed information of botmaster activities, it can be harmful if Botnet gets full control of the network [14]. Now-a-days, botmaster are

using many techniques to detect and avoid honeypots.

3. Analysis of DNS traffic: Though honeypots give information about botmaster's activities, it does not provide details of DNS query. Analyzing DNS traffic generated by bots and comparing them with normal DNS queries helps in detecting Botnet. Since new generation bots are designed to send minimum DNS queries, this technique is not useful for detecting new generation bot attacks [15].
4. Behavioral Analysis: For Botnet detection, few researchers have proposed behavioral analysis of network traffic. In this technique abnormal traffic patterns are instead of contents transferred over the network. This technique benefits in detecting unknown Botnet threats. The technique can analyze behavior actively or passively. In active analysis, bots' characteristics and behavior of attacks is closely monitored than other bot details like its behavior. This method is applicable for already established and propagated attack. While passive analysis is focused on bots' characteristics, C & C server, communication methodology, botmasters' behavior etc. The technique collects network traffic samples over a period of time and used to analyze Botnet behavior for detecting its existence in network [16].

V. Design of Botnet attack On Smartphone

Proposed bot code can be propagated through user involved vectors such as hiding itself into popular system applications like social networking app. Proposed research work design primarily focuses on the command and control channel and topology shown in the figure. In this, primary C&C communication will be transmitted via SMS messages and Bluetooth connection. These messages are disguised as spam to be less noticeable. The spam like messages usually encodes a command that asks the bot to send system info to particular server. Most secure topology to hide identity of botmaster is to user P2P topology of propagation. This allows botmaster and its zombie army to publish and search commands in a decentralized but organized fashion.

Objective of the research is not just to demonstrate that a mobile botnet can be stealthy, resilient but to discuss how to defend against botnet threat before it becomes serious. Mobile botnet cannot get to users phone without users' taking some action. So the first defense mechanism against botnet attack is user itself. User must take precaution before downloading and installing an application. Most of the applications downloaded on Android require strange permissions which are not required by the app.

For the development of botnet attack Android is selected as development platform for few obvious reasons. Gartner study released on November 2010 outlined that Android has become the second-most popular OS in the world. Android breakthrough on the smartphone market is due to several reasons: First, Android is an open-source Operating System unlike Apple iOS. Hence the other smartphone manufacturers have seen Android as an opportunity to turn the current users' keen interest for this open- source OS into a way to win market share [17]. In 2011, there was a mix of Android applications removed from the Android Market because they contained malware. There were over 50 infected applications - these applications were copies of "legitimate" applications from legitimate publishers that were modified to include two root exploits and a rogue application downloader [18]. In spite of the permissions-based security model implemented by Android, anyone can publish an application on the Android Market, which has no built-in method to detect if this application contains malicious code or not. This behavior has already been exploited several times in the past. "Droid09" attacked on mobile banking apps that seem to permit users to connect to their bank accounts, but in reality steal users' banking information. Derek Brown and Daniel Tijerina outlined how it is easy to publish an application and gain access to personal user data available on mobile.

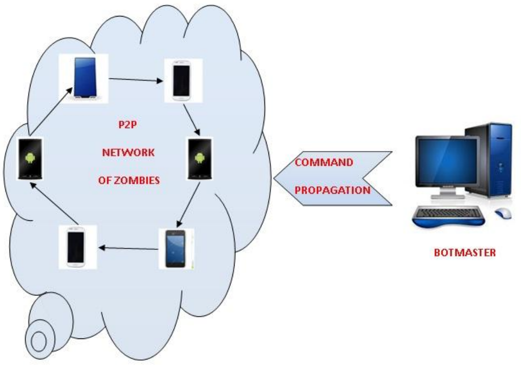

Fig 1: Botnet Design using P2P topology

VI. CONCLUSION

Today mobile phones are used everywhere, from trading on financial markets and mobile banking to carrying medical records, in weather forecasting to educational institutes etc. Though, every sector is not in need of strict security but every application needs security up to some extent. Many users are using online banking through mobile applications while patients are treated on medical diagnosis carried out using smart devices. If bot attacks on such mobile devices, it can create severe threats for the users and service providers. With the increased risk of new aged malwares, it is necessary for every smart device user to know the risk associated with it and protect device from malware attack. Though smartphone based botnet attacks are not as common as other malwares or PC botnet attack. But cyber criminals can easily exploit unawareness of mobile users to propagate botnet attacks.

This paper is focused on designing botnet attack using hybrid P2P architecture for propagation of mobile phone botnet attack thru SMS, Bluetooth and Online Social Medium. The purpose of designing botnet attack is to think like cyber attacker and malware developer as this is the first step towards providing security solution from attacks.

In further research work, we are going to detect botnet attack in early stage of its lifecycle and avoid its propagation further. Research work will also suggest safety measures which users must take while using smartphone. Along with users, network providers must take more precautionary actions to avoid botnet propagation and monitor unusual network activities and report them to cyber security professionals if possible.

REFERENCES

[1] Adeeb Alhomour, Irfan Awan & Jules Pagna Disso, “Towards An Enterprise Self-healing System against BOTNETs Attacks”, International Conference on Computing, Networking and Communications, IEEE 2013 Invited Positions Paper.
[2] Abdullahi Arabo & Bernardi Praggono, “Mobile Malware & Smart Devices Security : Trends, Challenges and Solutions”, 19th International Conferences on Control System and Computer Science, 2013, pp 526-531.
[3] Guining Geng, Guoai Xu, Miao Zhang and Yanhui Guo, Guang Yang, Wei Cui, *“The Design of SMS*
[4] http://security.radware.com/knowledgecenter/DDoSPe dia
[5]http://www.trendmicro.com/vinfo/us/security/definition/ commare and -and-control-%28c-c%29-server.
[6] http://searchsoa.techtarget.com/definition/bot
[7] Yuanyuan Zeng, “On Detection of Current and Next-Generation BOTNETs”, A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy (Computer Science and Engineering) in The University of Michigan, 2012.
[8] Collin Mulliner and Charlie Miller. Fuzzing the phone in your phone. In Black- Hat Security Conference, 2009.
[9] http://blog.cloudmark.com/2012/12/16/android-trojan-used-to-create-simple-sms-spam-Botnet
[10] Ihsan Ullah, Naveed Khan and Hatim Abolsamh, “Survey on Botnet : Its Architecture, Detection, Prevention and Mitigation”,IEEE 2013, pp 660 - 665
[11] Ping Wang, Sherri Sparks and Cliff Zou. “An Advanced Hybrid Peer to Peer Botnet”, IEEE Transactions on Dependable And Secure Computing, Volume 7, No. 2, April – June 2010.
[12] J. Goebel and T. Holz, "Rishi: Identify Bot Contaminated Hosts by IRC Nickname Evaluation," in *Proceedings of the First Conference on Hot Topics in Understanding Botnets*, 2007, pp. 8-20.
[13] J. S. Bhatia, R. K. Sehgal, and S. Kumar, "Honeynet Based Botnet Detection Using Command Signatures," *Advances in Wireless, Mobile Networks and Applications*, vol. 154, pp. 69-78, 2011.
[14] W. Zanoramy, A. Zakaria, and M. L. M. Kiah, "A Review on Artificial Intelligence Techniques for Developing Intelligent Honeypot," in *Proceedings of the 3rd International Conference on Next Generation Information Technology (ICNIT)*, Seoul: Korea, 2012, pp. 696-701.
[15] Meisam Eslahi, Rosli Salleh and Nor Badrul Anuar , “Bots and Botnets: An Overview of Characteristics, Detection and Challenges”, 2012 IEEE International Conference on Control System, Computing and Engineering, 23 - 25 Nov. 2012, Penang, Malaysia, pp 349-354.
[16] M. Bailey, E. Cooke, F. Jahanian, X. Yunjing, and M. Karir, "A Survey of Botnet Technology and Defenses," in *Proceedings of the Cybersecurity Applications & Technology Conference for Homeland Security (CATCH)*, 2009, pp. 299-304.
[17] Joany Boutet and Lori Homsher, *“Malicious Android Applications: Risks and Exploitation, How I Met All Your Friends, A Spyware story about Android Application and Reverse Engineering”*, Information Security Reading Room, The SANS Institute, pp. 1 – 5, 2 March 2010.
Based Heterogeneous Mobile Botnet”, Journal of Computers, Vol. 7, Issue 1, pp. 235-243, 2012.
[18] Abdullahi Arabo and Bernardi Pranggono, *“Mobile Malware and Smart Device Security: Trends, Challenges and Solutions”*, 19th International Conference on Control Systems and Computer Science, IEEE Computer Society, pp. 526-531, 10 – 11 September 2013.