Study of Mobile Botnets: An Analysis from the Perspective of Efficient Generalized Forensics Framework for Mobile Devices

Rizwan Ahmed
Research Scholar,
P. G. Dept. of Computer Science and Engineering,
G. H. Raisoni College of Engineering,
Nagpur, India

Dr. Rajiv V. Dharaskar
Director,
Matoshri Prathisthan Group of Institution,
Jijau Nagar, Off Latur Nanded Highway,
Nanded, India

ABSTRACT
Botnets represent a serious security threat on the Internet. Current security mechanism are typically inadequate for protecting against the latest breed of botnets, as botherders constantly develop new techniques and methods to frustrate investigators. Until recently, mobile networks have been relatively isolated from the Internet, so there has been little need for protecting against botnets. However, this situation is rapidly changing. With the rapid development of the computing and Internet access (i.e., using WiFi, GPRS and 3G) capabilities of smartphones, constructing practical mobile botnets has become an underlying trend. Thus, threats on the Internet most likely will migrate over to the mobile networks and vice versa. Botnets of malware injected into mobile devices will probably appear very soon, and there are already signs of this happening. This paper analyses the potential threat of botnets based on mobile networks. The study done will be further utilized for improving the performance of the developed "Efficient Generalized Forensics Framework for Mobile Devices". To conclude our paper, we suggest possible defenses against the emerging threat.

General Terms
Digital Forensics, Network Security, Mobile Network.

Keywords
Botnet, Security, Threat, Malware, Mobile Devices, Smartphone, MobileForensics.

1. INTRODUCTION
A Botnets [1] is a set of computers that are infected by a specific bot virus which gives an attacker (aka. Botherder or Botmasters) the ability to remotely control those computers. Most botnets are developed for organized crime where doing targeted attack to gain money. Example of attacks are sending spam [2], denial of service attack (DOS) or collecting and sale of information that can be exploited for illegal purposes. Researchers who fight against botnets are in general one step behind the attackers. Once they have found a solution to discover and take down a botnet the botherders change their botnet to fight back.

Botnet starts their lifecycle [2] when a vulnerability in an operating system or software are exploited or users have been fooled to run unwanted software on their computer. Malware is often distributed as spam within a malicious attachments, spam linked to infected websites, open file shares, through instant messaging (IM) or by scanning after vulnerabilities. Compared to older malware they spread much faster on the Internet than through floppy disk or Bluetooth. After exploiting the desktop computer a secondary infection that installs and updates the botclient appears.

Evolution of botnets has made them more difficult to discover [3] and take down because they hide their communication between the legitimate traffic on the Internet by using TCPport 80 [3] and they use peer to peer (P2P) technology that make them more resilient. Web based C&C [4] uses pull rather than push technology. Web servers can passively wait for the botclients to make contact. This lowers the network traffic between the botclients and the servers making it harder to spot the botnet on the network. To evade shutdown efforts the C&C needs to be constantly moving by using techniques like multihoming, fast flux and distributed C&C (Superbotnet). Waledac is a botnet on the Internet that is web based and communicates using XML messages as payload. MMS messages have a body field [5] where the XML message from Waledac can be hidden. Waledac can infect mobile devices and use MMS and SMS to communicate with its C&C.

2. MOBILE BOTNETS
Mobile devices are nowadays capable of using Internet connection [6], [7] through High-Speed Downlink Packet Access (HSDPA), Evolution-Data Optimized (EVDO), Universal Mobile Telecommunication System (UMTS), Enhanced Data Rates for GSM Evolution (EDGE) and General Packet Radio Service (GPRS) which are different IP based technologies evolved within the mobile network and wireless network (WLAN).

The term mobile botnet refers to a group of compromised smartphones that are remotely controlled by botmasters via C&C channels [8]. While PC-based botnets, as common platforms for many Internet attacks, have become one of the most serious threats to Internet, mobile botnets targeted for smartphones are not as popular as their counterparts for a variety of reasons including resource issues, limited battery power, and Internet access constraints, etc. Consequently, both the occurrence of practical mobile botnets and corresponding research on them are very limited. However, this could change with the recent surge in popularity and use of smartphones. Smartphones are now widely used by billions of end users due to their enhanced computing ability and efficient Internet access. Moreover, smartphones always store a large amount of sensitive personal data and are often used in online payment.

Therefore, smartphones have become one of the most attractive targets for hackers.

Since the appearance of Cabir, the first mobile worm (which was introduced in 2004), we have witnessed a significant evolution in mobile malware. Although the number of mobile malware has been growing steadily, their functionalities have remained simple until the development of the first mobile botnet in 2009. The mobile botnet, SymbOS.Yxes [9], targets Symbian and exploits a simple HTTP-based C&C. Later the same year, Ikee.B [10], which targets jailbroken iPhones and has a C&C mechanism similar to SymbOS.Yxes, was released. In December 2010, the first Android botnet, Geinimi, broke out mainly in China, still using similar HTTP-based C&C. Although advanced mobile botnets have not been witnessed in the main population of smartphones, we believe it is just a matter of time. Mobile botnets are presently posing serious threats for both end users and cellular networks [11]. Consequently, investigations into how mobile botnets work, as well as how they may be developed and stopped, represents an important area of research.

2.1 Mobile Botnets: Possible Attacks

Waledac is known for sending email [4]. An infected mobile device can send MMS or SMS to other mobile devices or to service numbers. Victims can be chosen by the botherder or they can randomly be chosen from the address book or contact list on the infected mobile device. These days there are many contests where you can vote for your favorite song, person, TV program and so on. A botnet consist of many infected computers and the voting system will not be able to detect if a botherder uses his botnet to send a short message to the voting service. But will anyone pay a botherder to vote up his or her favourite song or person? Maybe someone would in context of political elections [12]. Instead of using the voting application, a DDOS attack [3] against core of the mobile network can be done to stop people voting by making the voting system unavailable during the voting period.

There exist several service phones where you can give money to charity using mobile phones. If you call a specific service number the mobile device subscriber pays a preset amount or we can send an SMS to donate present amount for charity. One of the biggest examples where Americans used their cell phones to send text messages pledging more than $30 million for Haitian relief efforts [13]. What if a botherder creates his own service number and programs all his botclients to call that number. The price should be low so the subscribers would not notice and be suspicious about the extra charges [12].Mobile devices are being more common to our daily life. They are small and you can carry them everywhere you go and you will probably lose some of them too. Mobile devices can be used to communicate between people both through voice and messaging, play games alone or with others on the Internet, make payments, check the status on your bank accounts, store private information like contact information (name, phone number, email addresses), personal information (social security number, PIN codes, account numbers, private pictures or business related data) and other information that criminals can exploit and misuse for financial gain [14].

Infected mobile device will be able to act as spyware in the same way as botclient on desktop computers collecting personal information and send it to the attacker. Waledac is a plug-in based botnet and it is easy [4] to add plug-ins to extend functionality. There will be a possibility to create a plugin that scans the mobile device. The result can be reported back to the C&C in an XML document formed as an MMS.

Most people are trained to enter private data like credit card number, other sensitive personal and financial information on the mobile device using the mobile network while interacting with voice response system. Is this safe anymore as the traffic in UMTS and newer technologies are routed within the IP-network [15]?

2.2 Mobile Botnets: Challenges

There are several differences between smartphones and PCs. These differences lead to a number of challenges in the construction of a mobile botnet [11, 16]. (1). The battery power is rather limited on smartphones when compared with PCs. If the battery power consumption speed exceeds user expectations, the battery exhaustion is likely to be noticed by the user, leaving the bot open to detection. (2). The cost of smartphones is an extremely sensitive area for many users. If data costs begin to exceed the amount that the user had expected or agreed to pay, the bot could also be detected. (3). If C&C consumes an abnormal amount of network traffic, the abnormity is likely to be noticed. (4). The absence of public IP addresses and a constant change in network connectivity makes the robust P2P-based C&C in PC-based botnets impractical, and potentially impossible, in smartphones [8].

3. RELATED WORK

Botnets have been an active research topic in recent years. Current research on botnets is focused primarily on detection, measurement, tracking, mitigation, and future botnet prediction. Our research belongs to the last category. Wang et al. [17] presented the design of an advanced hybrid peer-to-peer botnet. Vogt et al. [18] presented a "super-botnet" - that works by inter-connecting many small botnets together in a peer-to-peer fashion. Ralf Hund et al. [19] introduced the design of an advanced bot called Rambot, developed from the weaknesses they found when tracking a diverse set of botnets. Starnberger et al. [20] presented Overbot, which uses an existing P2P protocol, Kademlia, to provide a stealth C&C channel. Singh et al. [21] evaluated the feasibility of exploiting email communication for botnet C&C. Nevertheless, few research works have studied how botmasters might design their advanced C&C for smartphones based botnets. Singh et al. [22] evaluated the feasibility of using Bluetooth as a medium for botnet C&C. We believe that this approach could be effective only when the mobile botnet is extremely huge (i.e., more than ten million), therefore, we focus our research on Internet based C&C. Mulliner et al. [16] proposed a SMS-HTTP hybrid C&C. The main idea of the hybrid schema is to split the communication into a HTTP and a SMS part. The encrypted and signed commands file is uploaded to a website and the corresponding URL is distributed via SMS. Zeng et al. [23] utilizes a SMS-based C&C with a P2P topology. Our work is complimentary to these approaches in that: (1). The SMS-based C&C (especially P2P topology) will inescapably cause excessive fees to users which leads to detection; and (2). The simple HTTP-based C&C scheme suffers a single-point-failure. As such, our study compliments this existing research, as we

have eliminated the single-pointfailure problem to some degree thanks to URL Flux.

4. MOBILE BOTNETS: DEFENSE MECHANISMS

We possibly should use following defense techniques against mobile botnets:

- Antivirus Scanning [24, 27]
- Intrusion Detection System (IDS) [24]
- Firewalls [27]
- Packet Filtering [24]
- Monitoring at SMSC [8]
- Infiltration [8]
- Building International Co-ordinated Mechanism [8]

Like Waledac [4] hiding its traffic through legitimated web traffic, Waledac on mobile devices can hide its traffic through legitimate MMS and SMS traffic making it harder for the researchers to spot botnets on the mobile network. Botclients communicate with each other and would adopt the same resilient behavior as botnets on the Internet. Waledac has a predefined structure on the messages. If you know what to look for there is possible to search and analyze the network traffic after specific signatures that Waledac or other known botnet creates. In front of email systems there may be an antivirus scanner that scans every incoming and outgoing email for malware. This requires extra resources, but may be necessary to protect end users against attack. MMS work in similar way as the email system where MMS messages is send from an MMS client to an MMS proxy server where it is converted to standard Internet MIME format to permit various media components to be carried over the Internet environment. The receiving MMS proxy server will convert it back to MMS format before delivering the message to the MMS server which stores MMS message. To protect users from spam and malware attack the mobile network operator should use an antivirus scanner in front of their MMS server scanning incoming and outgoing messages to stop malicious messages to be delivered to the end users.

Security on mobile devices are not safeguarded [14] in the same way as it is on desktop computers making the mobile devices easier to exploit. Compromised items inside a corporate network will constitute a threat since many security systems on the network can easily be bypassed. Mobile devices are often ignored. Jansen and Scarfone write in their article [14] that most corporate networks do not have centrally managed system to take care of the security policy and security update on mobile devices. It may also be difficult to update the mobile device due to lack of knowledge about how to do it. Many mobile device applications do not have update managers like applications on desktop computers do. A system is only as secure as its least secure component and mobile devices often fall into this category. To overcome this problem Janson and Scarfone [14] suggest several techniques. By using PIN codes the access to the SIM card is protected. Additional memory cards will not have the sama protection since they can be taken out and put into other devices. By turning off interfaces like Bluetooth, Infrared (IR), WLAN and other wireless access protocols until they are needed, the attack surface on the mobile device can be reduced. Install antivirus software can provide protection against incoming malware, but the application will drain battery power very fast. Use certificate based solutions to sign applications even if the newest worm Sexy Space [25] shows that this too is exploitable. Compared to malware and botnet evolution on the Internet, mobile platform are 7-8 year [26] behind. Experience from malware on the Internet can be transferred to malware on mobile device. Norman [26] predicts that malware on mobile device will evolve faster since techniques are already explored. Security mechanism on mobile devices therefore have to follow the same evolution as those on desktop computers. Windows Update for Windows Mobile devices exists already. Adobe Updater, Java Update Manager exists for desktop applications so why not implement these on mobile devices too? Some of these measures are also evolving on other latest mobile platforms as well.

5. FUTURE WORK AND CONCLUSION

Mobile devices are becoming more and more similar to desktop computers as smartphones continue to gain more capabilities. Mobile devices normally stay connected online all the time because of their default characteristics and user behavior. As a consequence of the integration of mobile networks into the Internet, security threats on one network will affect the other network. This makes smartphones the attractive targets to hackers. This opens the potential for botnets spreading to mobile networks. In the past the security of mobile networks has been relatively well controlled by the networks operators. By turning mobile devices into general purpose computation and communication platforms, new security vulnerabilities will emerge. The possibility of downloading Internet application to mobile devices also brings the risk of malware infection [28]. People need to become aware that mobile devices are vulnerable to being infected by malware, and thereby can be turned into a botclient as part of a botnet. In this paper we have shown that there are potential profitable business models for exploiting mobile botnets. It is therefore necessary to start thinking about methods for reducing the threat of botnets on mobile networks. We need to be well prepared for the promise attack, we, as defenders, should study mobile botnets attacking techniques that are likely to be developed by botmasters in the near future. To defend against such a mobile botnet, we suggest several possible countermeasures. In the future, we will invest more research on how to fight against this kind of advanced mobile botnet and relevant results will be used for improving the performance of the developed "Efficient Generalized Forensics Framework for Mobile Devices".

6. REFERENCES

[1] Norton. Bots and Botnets—A Growing Threat. Internet: http://us.norton.com/theme.jsp?themeid=botnet, read: 01.01.2012.

[2] Graig A. Schiller, Jim Binkley with Gadi Evron, Carsten Willems, Tony Bradley, David Harley, and Michael Cross. Botnets: The Killer Web App. Andrew Williams, Syngress, 2007.

[3] Kelly Jackson Higgins. Cellphone botnets, blackmailing voip and a healthy cybercrime economy. Darkreading, Oct 2008. http://www.darkreading.com/security/erabilities/showArticle.jhtml?articleID=211600782, read: 01.01.2012.

[4] Lasse Trolle Borup. Peer to peer botnets: A case study on Waledac. Master's thesis, Technical University of Denmark, Department of Informatics and Mathematical Modeling, System Security, Building 321, DK-2800, Kongens Lyngby, Denmark, 2009.

[5] Gwena¨el Le Bodic. Mobile Messaging technologies and services. Wiley and Sons Ltd, Second Edition, 2005.

[6] Sumit Kasera and Nishit Narang. 3G Mobile Networks. Architecture, Protocols and Procedure. Tata MCGraw-Hill Publishing Company, limited edition, 2005.

[7] Ajay R. Mishra. Advanced cellular network planning and optimisation: 2G/2.5G/3G ... evolution to 4G. John Wiley and Sons, 2007.

[8] Cui Xiang, Fang Binxing, Yin Lihua, Liu Xiaoyi, and Zang Tianning. Andbot: Towards Advanced Mobile Botnets. http://www.usenix.org/event/leet11/tech/full_papers/Xiang.pdf , read: 01.01.2012.

[9] Axelle Apvrille. Symbian worm Yxes Towards mobile botnets. http://www.fortiguard.com/papers/EICAR2010_SymbianYxes_Towards-Mobile-Botnets.pdf, read: 01.01.2012.

[10] P.A. Porras, H. Saidi, V. Yegneswaran, "An Analysis of the iKee.B iPhone Botnet," in Proceedings of the 2nd International ICST Conference on Security and Privacy on Mobile Information and Communications Systems (Mobisec), May 2010

[11] P. Traynor,M. Lin, M. Ongtang, V. Rao, T. Jaeger, T. La Porta and P. McDaniel, "On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core," in ACM Conference on Computer and Communications Security (CCS), November 2009

[12] Anne Ruste Flø and Audun Jøsang. Consequences of Botnets Spreading to Mobile Devices. Proceedings of the 14th Nordic Conference on Secure IT Systems (NordSec 2009). Oslo, October 2009.

[13] Suzanne Choney. Mobile giving to help Haiti exceeds $30 million,http://www.msnbc.msn.com/id/34850532/ns/technology_and_science-wireless/t/mobile-giving-help-haiti-exceeds-million/#.TwCVetSP-7Y, read: 01.01.2012.

[14] W. Jansen and K. Scarfone. Computer security, guidelines on cell phone and pda security. Technical report, NIST- National Institute of standards and Technology, US Department of Commerce, 2008. Special Publication 800-124.

[15] Jr Raphael. Botnet spam attacks to target cell phones. PC World, Internet, Oct 2008. http://www.networkworld.com/news/2008/101608-report-botnet-spam-attacks-to.html, read: 01.01.2012.

[16] C. Mulliner, J.P. SeifertIn. Rise of the iBots: 0wning a telco network. In the Proceedings of the 5th IEEE International Conference on Malicious and Unwanted Software (Malware) Nancy, France 19-20 October, 2010.

[17] P. Wang, S. Sparks et al. An advanced hybrid peer to peer botnet. Proc. of the HotBots'07, First Workshop on Hot Topics in Understanding Botnets, Cambridge, MA, 2007.

[18] R. Vogt, J. Aycock, and M. Jacobson, "Army of botnets," Proc. of 14th Annual Network and Distributed System Security Symposium (NDSS'07), 2007.

[19] R. Hund, M. Hamann and T. Holz. Towards Next-Generation Botnets. Proc. of the fourth European Conference on Computer Network Defense (EC2ND 08), 2008.

[20] G. Starnberger, C. Kruegel, and E. Kirda, "Overbot - a botnet protocol based on kademlia," in Proc. of the 4th Int. Conf. on Security and Privacy in Communication Networks (SecureComm 08). September 2008.

[21] Kapil Singh, Abhinav Srivastava et al. Evaluating Email's Feasibility for Botnet Command and Control // Proceedings of The 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2008). Anchorage, Alaska. June 2008.

[22] K. Singh, S. Sangal, N. Jain, P. Traynor and W.Lee, "Evaluating Bluetooth as a Medium for Botnet Command and Control," in Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA), July 2010.

[23] Yuanyuan Zeng, Xin Hu, Kang G. Shin, "Design of SMS Commandedand-Controlled and P2P-Structured Mobile Botnet", The University of Michigan, Ann Arbor, MI 48109-2121, U.S.A. 2009

[24] Yan Zhang, Jun Zheng, and Miao Ma. Handbook of Research on Wireless Security. Idea Group Inc (IGI), 2008.

[25] Irfan Asrar. Could sexy space be the birth of the sms botnet? Symantec, Internet blog, July 2009. http://www.symantec.com/connect/blogs/could-sexy-space-be-birth-sms-botnet, read: 01.01.2012.

[26] Norman ASA. Mobile phone threats - hype or (finally) truth? Security Articles- Archive, 2009. http://www.norman.com/security_center/security_center_archive/2009/67174/en, read: 01.01.2012.Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[27] Neal Leavitt. Mobile Security: Finally a Serious Problem?, 2011, http://www.leavcom.com/pdf/Mobilesecurity.pdf , read: 01.01.2012.

[28] Jim Giles, Sneaky app shows potential for smartphone botnets, March 2010, http://www.newscientist.com/blogs/shortsharpscience/2010/03/mobile-botnets-threaten-smartp.html?DCMP=OTC-rss&nsref=online-news, read: 01.01.2012.