All Bot Net: A Need for Smartphone P2P Awareness

Kelly A. Cole, Ramindu L. Silva, and Richard P. Mislan

CERIAS
Purdue University
West Lafayette, Indiana, IN 47907, USA
{kcole,rsilva,rick}@purdue.edu

Abstract. This paper is a call for law enforcement and other members of the digital forensic community to be aware of smartphones connecting to Peer-to-Peer networks. This paper also offers a review of botnet concepts and research surrounding smartphone malware.

Keywords: Botnet, Peer-to-Peer (P2P), Smartphones, Computer Forensics, Cyber Forensics, Law Enforcement, Cybercriminals, Malware.

1 Introduction

Internet penetration around the world has increased at an incredible pace. Along with this availability, there has been a proliferation of internet ready devices. Most, if not all of these devices are potential targets for malicious software (malware) which can infect and compromise devices and data without the owner's knowledge. One of the payloads malware is capable of delivering is code that makes the device a part of a botnet. A botnet is "a network of compromised computers that can be remotely controlled by an attacker" [1].

In order to better understand botnets, some terminology must be defined. Compromised computers are referred to as "drones", "zombies", "infected nodes" or "infected hosts". The people who manage the drones are known as "bot herders" or "bot masters" and the malicious software that is loaded onto a victim's computer is called a "bot" [2].

In order to build a botnet, the bot master will release malware with a bot payload designed to infect as many devices as possible. The potential power and effectiveness of the botnet is primarily determined by the number of drones contained within it. The more drones a bot master accumulates, the more powerful the resulting botnet becomes [2].

Bot malware can be spread to a computer or device in a number of ways. It can be embedded in an e-mail attachment, or it could enter through downloading infected files from a peer-to-peer network. Bot malware can also be spread through scripts running on infected web sites; automatically downloading and infecting the victim's computer when they visit a malicious website [2].

Section 2 of the paper provides a brief history of the evolution of botnets. Section 3 discusses Peer-to-Peer applications currently available for various smartphone platforms. Section 4 presents multiple attack vectors that can be utilized to

P. Gladyshev and M.K. Rogers (Eds.): ICDF2C 2011, LNICST 88, pp. 36–46, 2012.

compromise a smartphone. Section 5 identifies some reasons why botnets are, and will continue to be, attractive to cybercriminals. Section 6 shows the importance of seizing all internet capable devices, including smartphones, when processing a crime scene. Finally, Section 7 outlines a possible new line of attack for smartphones.

2 Botnets

There are four main types of botnets, distinguished by the way the drones receive commands from the bot master. They are:

- Centralized IRC Command & Control botnets
- Centralized P2P botnets
- Decentralized P2P botnets
- Hybrid P2P botnets

2.1 Centralized IRC Command and Control Botnets

Once the bot malware has infected a victim's computer, it is designed to connect the drone to a specific IRC channel on a pre-determined IRC server [3]. The bot master can then connect to the IRC channel and issue commands to the drones [4]. Since the bot master only needs to communicate with the IRC server to control the botnet, they can perform attacks rather anonymously, from practically anywhere. Bot masters can use anonymizing technologies such as the Tor network to hide their Internet Protocol (IP) address, making it difficult for authorities to trace should the botnet server be seized and investigated [3]. Tor is a freeware application that attempts to anonymize your internet communications by rerouting your traffic through a network of computers around the world, thereby hiding the original source.

The above design is known as a centralized IRC Command and Control (C&C) design because all the bots point to a single server for instructions [1]. The primary flaw in this design is if the central server is shut down by the authorities, the botnet can no longer be controlled. Researchers have found that cybercriminals are discontinuing the use of centralized IRC C&C servers in favor of decentralized Peer-to-Peer (P2P) communication [1].

2.2 Centralized P2P Botnets

P2P technologies became attractive to attackers for setting up botnets with the release of Napster, which was the first P2P file sharing service, designed for users to share audio files directly with one another. Napster used a centralized P2P design; meaning it functioned with a central server that maintained lists of connected users and files. When Napster was deemed illegal, the Gnutella protocol was developed with fully decentralized P2P services [5].

2.3 Decentralized P2P Botnets

In a Gnutella network, each user node (peer) in the network functions as both a client and a server [1]. When a node performs a search, the query is forwarded from node to

node and routed towards the host most likely to have the requested file [6]. While Gnutella relied on flooding every node on the network to locate files, newer protocols such as Chord and Kademlia use a distributed hash table (key, value pairs) to locate files on the network [5].

2.4 Hybrid P2P Botnets

Kazaa is an example of a hybrid P2P model, combining the benefits of both the centralized and fully decentralized approaches. This "semi-centralized" network essentially takes a decentralized model and creates smaller sub-networks, each with a central server known as a "super-peer". Each super-peer maintains a list of files hosted within its sub-network and shares that information with other super-peers. When a peer performs a search, it is sent to the super-peer which first checks if that file is available within its own sub-network. If not, the request is forwarded to another super-peer which then repeats the process. Once the file is located, it is transferred directly to the requesting peer from the host [6].

These distributed P2P networks are inherently attractive to attackers wishing to deploy a botnet due to the elimination of a centralized server, making it much harder for authorities to destroy the botnet.

The following example of how P2P botnets operate is just one of many ways in which P2P botnets can be deployed. In this example, a device is infected when the user opens an email attachment infected with malware containing the bot payload. Once the device is infected, the bot publishes itself on the P2P network and then attempts to connect to the initial list of hardcoded peers. The bot master will then push secondary commands for the bot (injections) to the P2P network [5]. The bot will then instruct the drone to automatically download these injections. This system provides the communication channel from the bot master to the drones, eliminating the need for a centralized server. The bot on the infected device can be designed to update itself by connecting to any recently updated node on the network [5].

3 Smartphone P2P Networks

The BitTorrent protocol is currently one of the most popular decentralized file sharing technologies in use on the Internet, largely as a result of its speed. Unlike the previous P2P file sharing technologies discussed earlier, BitTorrent networks require ancillary support to search for files and peers. The BitTorrent protocol divides files into small pieces or segments, and once a user downloads a particular segment, it is automatically hosted by the user for other. By distributing these segments to multiple hosts, more users are able to download large files quickly [7]. To ensure the authenticity of all of the individual segments, an SHA-1 hash value is calculated for each segment and is stored in the torrent descriptor [8].

SymTorrent and GridTorrent are full featured BitTorrent client applications for smartphones running the Symbian OS [7]. SymTorrent has been downloaded over half a million times. It uses the standard BitTorrent protocol and therefore downloads

files to the smartphone in the same way as a computer. SymTorrent uses a central server or "tracker" that maintains a list of peers. When a peer starts downloading a torrent, it connects to the server and announces its address. The server will then provide a list of peers currently downloading and sharing that particular torrent, also known as the "swarm". The peers communicate with the tracker via standard HTTP GET requests. The newest version of BitTorrent supports tracker-less torrents which hashes a peer's address by using a Kademlia algorithm [7].

GridTorrent is a similar, yet more efficient version of SymTorrent. GridTorrent has added features that allow users to form small local networks using either Wi-Fi or Bluetooth. Although limiting the number of accessible peers, it allows users to transfer large files without incurring cellular data charges [7].

Symbian OS smartphones also have access to an application called Symella which connects users to the completely decentralized Gnutella P2P file-sharing network [9]. Users can search and download files using Symella; however they are not able to share files on the network due to limitations of the smartphone [6].

Mobile P2P services and applications are still developing and continue to improve in performance and features. Many mobile P2P systems use an overlay network to existing network infrastructures so that devices such as smartphones can connect to the P2P network. For instance, JXTA, an open source P2P protocol, allows any device including smartphones and PDAs to connect to a network exchange data regardless of the underlying network infrastructure [10].

Heikkinen, Kivi and Verkasalo [11] analyzed GSM/UMTS traffic of three major cellphone carriers in Finland. In the traffic trace measurement, they identified P2P file sharing traffic based on TCP/UDP port numbers and used TCP fingerprinting to differentiate between computers and cell phones. BitTorrent and eDonkey were the most popular protocols in use among smartphone users. Fring, a P2P mobile Voice-Over-IP (VoIP) client, was the only client found to have significant usage and data volume levels. This study shows that P2P file sharing on smartphones is a reality, but is still in its infancy.

4 Botnet Attacks Using Mobile Phones

Research has found that cellular networks can host a botnet attack. Short Message Service (SMS), Multimedia Messaging Service (MMS) and Bluetooth are the most common attack vectors to infect a smartphone [12]. Infected e-mails, applications and web pages have also been shown as viable methods of infecting smartphones with malware.

4.1 Peer-to-Peer and SMS

Attacks that enter into a phone through an SMS message are known as Smishing [13]. SMS is one of the most frequently used modes of communication in the world. It is also the most popular method used by attackers to send out spam and to set up a botnet C&C channel on a smartphone [14].

Zeng [14] developed a mobile botnet proof of concept that uses SMS to transmit C&C messages and uses a decentralized P2P network that allows bot masters and bots to publish and search for commands. The researchers were able to hide malicious SMS messages from the user by marking it as spam. This resulted in the message bypassing the inbox and going directly to the spam folder where it issued commands to the phone. Even if a user manually deleted the spam, the code still executed when it was received.

For the P2P component, the researchers chose Kademlia which uses distributed hash tables for finding information in P2P networks. Under Kademlia, the bot master can publish commands on the P2P network and bots can actively search for these commands. Each node in the network has an ID which is composed of a 128 bit hash function and a key. Nodes find each other with these IDs and only exchange data with a node that has the data item associated with their key [14].

The researchers presented a slight twist similar to the Chord protocol, where a node ID is the hash of its IP address. Instead of issuing node IDs as randomly generated hash functions, they hashed the node's phone number. They used a symmetric key algorithm, AES, to conceal the hashes from being identified as phone numbers by authorities. Each bot also stored the AES keys so that it could decrypt the commands. Some critical commands sent by the bot master such as "SEND SPAM" were encrypted while commands for P2P communication such as "FIND NODE" were concealed without full encryption [14].

4.2 SMS/MMS and Email

Attempts to build botnets through SMS have been documented in the real world. According to Symantec, a malicious SMS titled "Sexy Space" was released in 2009. When opened, it tricked the victim into downloading malicious software which then connected the phone to a botnet. Symantec found these phones to be connected to a central server on the Internet but were unsure if they were receiving remote commands [15]. This attack targeted Nokia's S60 3rd edition software platform running on the Symbian OS [16].

The Zeus or Zbot botnet variants are usually associated with electronic banking attacks targeting small businesses. They are reported as one of the most threatening malware in regards to data theft in the world today [17]. Zbot now has a mobile version, called Zeus mobile or Zitmo, to collaborate with its computer based component. Zitmo targets smartphones running on the Symbian OS, Windows Mobile and Blackberry OS [18].

First a victim's computer is infected with the Zitmo malware through one of many attack vectors, for instance downloading an infected email attachment. The malware then modifies a legitimate bank website on the victim's computer by injecting a new dialog asking for the user's cell phone number and model during the login process. Once submitted, an SMS message is sent to the user's smartphone with a URL link which is really a version of Zeus customized for that particular user's smartphone model [18].

Once Zitmo is installed on the smartphone, it configures a C&C phone number to which all incoming and outgoing SMS messages are forwarded. The purpose of this is to intercept the confirmation SMSs sent by banks to their customers [18].

Smartphones running Symbian OS spread the Trojan as a SISX file named "cert.sis". The installation package is issued to "Mobil Secway" and it is signed by Symbian CA [19]. By default, Symbian smartphones are not set to validate certificates online. Even if Symbian revoked the certificate, smartphones that have this feature disabled will not warn the user of the invalid certificate [19].

4.3 MMS/Email

There are many ways of deceiving individuals into clicking infected links. Attacks through email and MMS are similar to SMS attacks where malware can enter a cellphone through the user clicking on the MMS picture or link. The most deceitful attacks are those that appear to originate from a known source, also known as "spear phishing". For instance, the source of the infected email looks like it is coming from an employee within the recipients own company [13].

Spam emails with infected attachments are sent to smartphones with the help of computer botnets. Since smartphones run on a variety of operating systems, multiple versions of the malware must be sent within the malicious attachment to ensure the correct code is executed [14]. In addition to these threats, the free Wireshark packet sniffer program can sniff smartphone email packets to reveal private email content [20].

4.4 Bluetooth

Bluetooth is a radio communication standard that operates in the 2.4GHz band and is used for short-range communication between Bluetooth compatible devices [7]. Many Bluetooth vulnerabilities have been discovered and documented. Bluetooth is susceptible to backdoor attacks, allowing an attacker to gain access to contact lists, SMS history and other data stored on the phone. BlueSnarf is one such tool that bypasses the normal Bluetooth paring procedure, allowing private information to be captured without the victim's knowledge.

Recent research has shown that many smartphones have vulnerabilities that allow backdoor access to the phone and its data [21]. For instance, FlexiSPY, an application sold online for "catching cheating spouses", is available for Symbian, Windows Mobile, Android and BlackBerry. It offers location tracking through GPS information and remote listening [22]. An attacker can view the phonebook, call logs and all incoming and outgoing text messages. All of this information is uploaded and stored on a secure FlexiSPY account. The software would have been classified as malware if it was not for the fact that it lacks the ability to self-install, and also does not perform any key-logging [22].

A couple of other Bluetooth hacking tools that exist are BlueBug and Blue Smack. BlueBug, which is based on ASCII Terminal (AT) commands, allows the attacker access to most of the features and data of the smartphone [21]. Blue Smack allows an

attacker to launch a Distributed Denial of Service (DDoS) attack using a Ping of Death attack but with Bluetooth technologies [21].

According to Singh, Sangal, Jain, Traynor and Lee [23], control messages can be sent through Bluetooth channels to infected cell phones or nodes. In their study a model bot was coded in Java and deployed on the Sun Wireless Toolkit that emulated infected cell phones. Upon infection, the bot registered itself through Bluetooth using the Universally Unique Identifier (UUID) of the infected phone, which allowed it to be discovered by other infected Bluetooth devices. As infected phones passed within Bluetooth range of each other, they exchanged identity information and the most up-to-date bot would update the other device if necessary. After a threshold of recordings, the most popular nodes (nodes with the highest exposure to other bots) sent their logs to the bot master, identifying which phones were in the botnet and which phones were the most popular. Only the most popular nodes communicated with the bot master directly. The researchers included a command that directed all the bots to send an SMS to a specific mobile number without being noticed by the sender. This command could result in a DDoS attack if the botnet had enough drones.

This proof of concept study shows that for a Bluetooth based botnet to succeed, the infected cellphones must frequently be within Bluetooth range of each other and the bot master's device in order coordinate an attack [23].

4.5 Mobile Applications

Many smartphones currently have application stores. Users who download these applications face the threat of embedded malware. The operating systems Android and BlackBerry OS bundle user confirmation and signature permissions within its applications in an attempt to halt malicious third-party applications from being downloaded [22]. Also, certification authorities, such as SymbianSigned and Apple, provide source code inspection services; however this process is not perfect and malicious applications do get through. Some OS based control policies are not as strict as others, allowing developers to sign their own applications. For instance Android based cell phone applications are not well controlled when compared to other platforms [22]. The iPhone application control policy is on the strict side but it cannot protect modified or "jailbroken" iPhones from malicious third party applications [14]. Most smartphones require user acknowledgement before they allow any software to install [22]. However, as is the case with computers, a user can be deceived into installing what appears to be legitimate software or accepting a security certificate from a questionable source.

Tijerina and Brown [24] developed two identical looking smartphone applications, one performed as advertised, but the other contained code that turned the smartphone into a bot. As a proof of concept, the legitimate version was made available on the iOS and Android platforms and heavily promoted. Their study demonstrated how easy it would be to gather cell phones to be used in a botnet by offering a legitimate looking, but malicious cell phone application to the public. They had 20,000 individuals view the legitimate application, and over 8,000 people downloaded it to their phones. Had they released the malicious version of the software, those 8,000

smartphones would now be a part of a smartphone botnet. Since the malicious version of the application was never released, it is unknown if it would have passed Apple's code review process.

4.6 The Internet (Wi-Fi and 3G)

A recent study has found that 38 percent of adult smartphone users use their phone to surf the Internet, making web browsing more popular than the use of other applications [25]. As with computer based web browsing, smartphone users should be aware of attacks that can happen while surfing the web with a smartphone. Attackers can insert scripts that do not alter the appearance of a website, but could redirect the victim to another web site that may cause malware to be downloaded to the smartphone [21].

A browser exploit has been discovered on the iPhone that exposes the user's phonebook, call history, SMS history and voice mail data when they visit certain malicious websites. This information can then be sent to the attacker. This malicious code could also be designed to send text messages to the user, that when clicked, would sign the user up for pay service to rack up charges to the user's account [20].

Although smartphones use different operating systems that vary in terms of design, functionality and network stack architecture, according to Khadem [21], they all have the following common features:

- They all support different cellular standards such as GSM/CDMA and UMTS to access cellular networks.
- They can access the Internet through different network interfaces such as Bluetooth, WLAN (IEEE 802.11), infrared and GPRS, and have a TCP/IP protocol stack for connection to the Internet.
- They can be synchronized with desktop PCs.
- They are able to multi-task and run multiple applications simultaneously.
- They have open APIs (Application Programming Interface) to develop 3rd party applications.

Khadem [21] evaluated the network stack of Symbian OS and Windows Mobile 5.0 smartphones lacking antivirus protection and firewalls. He found that after using network scanning and packet sniffing applications such as Nmap and Wireshark to scan and capture network packets, the TCP and IP header and the network stacks architecture of the Windows Mobile 5.0 platform was similar to those of the PC based Microsoft Windows OSs. Therefore, the same vulnerabilities in Windows PCs could potentially be exploited on smartphones running Windows Mobile [21]. The majority of botnets are composed primarily of Microsoft Windows based computers, so cybercriminals are already familiar with many of the vulnerabilities that could be exploited to create a smartphone botnet [26].

When looking at vulnerabilities of the Symbian based smartphones, Nmap was able to find the IP address, MAC address and all open/closed/filtered port. Also when using a fingerprinting technique one could check which operating system is running

on the device and find out more information about the network stack architecture for reconnaissance [21]. Symbian smartphones were also found to be vulnerable to ARP spoofing attacks [21].

5 Why Are Botnets Attractive to Cybercriminals?

One of the most common uses of a botnet is to anonymously create and send spam emails. The FBI stated that botnets currently send up to three-quarters of all spam messages [27]. A bot master can command all of the drones to forward spam emails or phishing scams to third party victims [28]. Bots can also be designed to forward malicious links to the contacts listed in the drone computer's instant messaging and email accounts [28]. The spam and other malicious messages appear to originate from the victims, allowing the bot master to remain anonymous.

DDoS attacks are another common use of large botnets. In this type of attack, a bot master will instruct the drones to send small network requests to a server or device. If the botnet has enough drones, the sheer volume of requests coming into the server or device will either cause it to crash or slow to a crawl [28].

Smartphones, with their ever increasing processing power and 24/7 internet access capabilities, are becoming more and more attractive targets for cyber criminals. These devices are essentially becoming handheld computers capable of conducting online banking, shopping, email, instant messaging, web browsing, downloading applications and connecting to P2P networks. All of the popular smartphone platforms such as Microsoft's Windows Mobile, Nokia's Symbian, Google's Android, Apple's iOS and RIM's Blackberry OS offer these features, making them at risk to a range of attacks [23].

6 Smartphone P2P Investigations

P2P networks are the most popular way for criminals to distribute child pornography. BitTorrent and Gnutella protocols used by client applications like Morpheus, Symella, Shareaza Frostwire, Limewire, Phex and BearShare are found to be the most widely used among child pornography (CP) users [29]. Authorities are able to detect P2P users downloading illegal content by identifying hash functions associated with the image or video, IP address and Globally Unique Identifier (GUID) associated with the account [29]. An application called RoundUp is used by Law Enforcement (LE) to investigate Gnutella networks and identify files with known hash values. It is used by 52 Internet Crimes Against Children (ICAC) Task Forces in the U.S. [8]. When using RoundUp, LE is unable to distinguish between a smartphone and a computer because all activity on the P2P network looks the same. This is important to keep in mind when conducting a search on a P2P case. If no evidence is found on the suspect's computer and the suspect had an unsecured wireless access point, LE may assume a third party may have downloaded the illegal content by "borrowing" the internet service from the suspect. However, it is now conceivable that the suspect could have

been using their smartphone to download the illegal content from the P2P network; therefore examination of all such devices at a crime scene is crucial.

7 Proposed New Line of Attack

The proposed cell phone botnet attack design makes it possible for security researchers to investigate and develop new countermeasures for this coming attack.

In the study, an enticing phone number is posted on popular social networking websites such as Facebook, MySpace and Craigslist, offering a free product. When a smartphone user clicks on this phone number, their phone not only calls the VoIP (Google Voice) number but their browser connects them to a web server in the background. Most users will not see the phone connect to the web server because they will be talking on the phone by this point. The number of calls received by the VoIP number will serve as an indication of the number of potentially compromised smartphones.

8 Conclusion

The popularity of smartphones shows no signs of slowing. According to Gartner [30], worldwide smartphone sales increased 96 percent from the previous year, accounting for 19.3 percent of the 417 million cellphone sales for that period. As these devices become more prevalent, they will increasingly become targets of malicious attacks [14]. It is therefore imperative that these devices are hardened to thwart as many threats as possible. Symantec and other researchers in the field are recommending that smartphones be secured to the same levels as computers. Antivirus protection, anti-spam for SMS, a firewall, and data encryption technologies are all advised to help minimize the threats explored in this paper [13].

The increasing power and functionality of smartphones has resulted in criminals using these devices to conduct various crimes. Technologies like mobile P2P are still in its infancy, but will undoubtedly become more popular in the future. Law enforcement should be cognizant of the capabilities of smartphones and should not overlook them when conducting digital forensic examinations.

References

1. Holz, K., Wicherski, B.: Know your Enemy: Tracking Botnets. The Honeynet Project (2008)
2. Long, D.: The Lazy Person's Guide to Botnets. In: CHIPS (2008)
3. Shadowserver: Botnets. Shadowserver (2009)
4. Skoudis, E.: Liston.: Counter Hack Reloaded. Pearson Education, Inc., NJ (2006)
5. Grizzard, J.: Peer-to-Peer Botnets: Overview and Case Study. The Johns Hopkins University Applied Physics Laboratory (2007)
6. Lehtinen, J.: Secure and Mobile P2P File Sharing. In: TKKK (2006)

7. Fitzek, F.H.P., Charaf, H.: Mobile Peer-to-Peer Networks: An Introduction to the Tutorial Guide. Wiley (2009)
8. Liberatore, M., Erdely, R., Kerle, T., Levine, B.N., Shields, C.: Forensic investigation of peer-to-peer file sharing networks. In: Digital Investigation (2010)
9. Dybwad, B.: Symella: a Gnutella client for Symbian smartphones. In: AOL (2005)
10. Srirama, S.N.: Publishing and Discovery of Mobile Web Services in Peer to Peer Networks. In: German Research Foundation, DFG (2010)
11. Heikkinen, M.V.J., Kivi, A., Verkasalo, H.: Measuring Mobile Peer-to-Peer Usage: Case Finland. TKK Helsinki University of Technology (2007)
12. Fuentes, D., Álvarez, J., Ortega, J., Gonzalez-Abril, L., Velasco, F.: Trojan horses in mobile devices. In: ComSIS (2010)
13. Symantec: The Need for Multi-Channel Security, http://www.symantec.com/business/resources/articles/article.jsp?aid=20091110_multi_channel_security
14. Zeng, Y., Hu, X., Shin, K.G.: Design of SMS Commanded-and-Controlled and P2P-Structured Mobile Botnets. The University of Michigan (2010)
15. Asrar, I.: Could sexy Space be the Birth of the SMS Botnet? Symantec Corporation (2009)
16. InfoNIAC: Get Ready for Cell Phone Botnets, http://www.infoniac.com/hi-tech/get-ready-for-cell-phone-botnets.html
17. Baylor, K., Brown, C.: TrendMicro: The Threat Defined. Killing Botnets. McAfee (2006), http://community.trendmicro.com/t5/Web-Threat-Spotlight/ZBOT-Zeus-Sends-Out-Tailor-Made-Spam/ba-p/1245
18. Polska, C.: ZITMO: The new mobile threat, http://www.cert.pl/news/3193/langswitch_lang/en
19. McAfee: SymbOS/Zitmo.A. McAfee, Inc. (2011)
20. Hoffman, D. V.: Smartphone Hacks and Attacks: A Demonstration of Current Threats to Mobile Devices. SmobileSystems (2008)
21. Khadem, S.: Security Issues in Smartphones and their effects on the Telecom Networks. Chalmers University of Technology (2010)
22. Enck, W., Ongtang, M., McDaniel, P.: On Lightweight Mobile Phone Application Certification. In: CCS (2009)
23. Singh, K., Sangal, S., Jain, N., Traynor, P., Lee, W.: Evaluating Bluetooth as a Medium for Botnet Command and Control. Springer, Heidelberg (2010)
24. Tijerina, D., Brown, D.: Is that a bot in your pocket? Or does it just look like one? TippingPoint's DVLabs (2010)
25. Randow, A.: Touring the Mobile Market: why native apps are not the solution for the mobile universe. TourSphere (2010)
26. Liu, J., Xiao, Y., Ghaboosi, K., Deng, H., Zhang, J.: Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures. EURASIP Journal on Wireless Communications and Networking (2009)
27. FBI: The Case of the "Zombie King". Federal Bureau of Investigation (2009)
28. Baylor, K., Brown, C.: Killing Botnets. McAfee (2006)
29. Liberatore, M., Levine, B.N., Shields, C.: Strengthening Forensic Investigations of Child Pornography on P2P Networks. ACM (2010)
30. Gartner: Gartner Says Worldwide Mobile Phone Sales Grew 35 Percent in Third Quarter 2010; Smartphone Sales Increased 96 Percent. Gartner (2010)