International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Exhaustive Comparison and Analysis of Botnet Attacks for Smartphones

Dr. Sonali Kothari*[1], Dr. Shubham Joshi[1], Ishaan Tidke[2]

Submitted: 16/09/2023 **Revised**: 17/11/2023 **Accepted**: 29/11/2023

Abstract: Different researchers have proposed different methods for designing botnet attacks using varying C & C channels. During earlier research in field of botnet, researchers worked on developing botnet attacks more than their detection. This helps in identifying methodologies employ for designing botnet attacks. With different communication methods, botnets were first designed for PCs. But with changing era researchers and cyber criminals are looking for methods for developing and understanding smartphone based botnet attack. Besides developing botnets for PCs and smartphones, researchers and security organizations are working for identification of different mobile phone botnet attacks. In the present article, study of existing literature is discussed to understand the history of botnet attacks and various methods evolved. The survey discusses different players of botnet attacks; different topologies evolved and various modes of propagation along with C&C channel. The chapter also includes practices and concepts of botnet attack, performance evaluation measures and databases used by various researchers. Literature survey also highlights some real botnet attacks used for commercial purpose or steal information using various platforms.

Keywords: *Botnet, Mobile Security, Android Security, Command and Control Serve, Botnet Attack*

1. Introduction

Over the last two decades, the Internet has grown into a significant infrastructure, with millions of users conducting a wide range of everyday operations through it. To carry out daily business and provide services to customers, many of enterprises rely on the Internet. In the same time frame, cybercriminals began posing dangers towards the Internet, making its security a serious concern. The characteristics of the Internet that helped it develop—features like each node's ability to run arbitrary code—became targets and were utilized for cybercrime, carrying out unlawful acts on a large scale.

These actions result in billions of dollars in worldwide damages. The Internet must be secured against such harmful activity. Many researchers are now striving to secure the internet. The technical diversity of internet security is what makes it such a crucial topic for researchers. The internet cannot be sufficiently secured using only technical means. Many techniques have been offered in previous years to prevent DoS (Denial of Service) attacks. However, none of them have been able to guarantee ongoing security. Cybercriminals always develop new ways to strike. Although the current remedies haven't fully failed, they do need to be updated or improved in light of the new threat. Similar rules apply to other types of online applications.

Among all these online threats, botnet is emerged as one of the hardest attack to handle. Botnet (network of bots or zombies) comprises of three main components - bots, Command and Control (C & C) servers and botmaster. A bot is a compromised computer system which runs malicious code to infect other computes in its network and infect them without knowledge of owner and in association with other compromised computes. C & C server is the communication channel between bots and botmaster. C & C server receives malicious code from botmaster. It is the responsibility of C & C to propagate the malicious code to infected bots and spread it to other computer systems to infect them. Command and Control server does the job of spreading commands/attacks to various devices and creating network of bots (victim devices). Botmaster is the administrator of the botnet. Botmaster sends malicious code to C & C server and remain hidden behind it. Botmaster keeps track of activities performed by C & C, maintains details of all C & C and infected bots. Once botmaster get access to any device, it can control its activities without knowledge of user through C & C server.

The basic necessity was listed earlier as: living space, clothing and foods; however as the global market evolved and renewed itself, the necessity of technology and communication grew along and widened. Now the same basic necessity has been modified as food, clothing, shelter and technology. The impact technology has created from late 90s till current date can be mentioned as the impact of the technology era. Mainly, the communication and information has achieved a greater and sustainable place in the global aspect. ICTs (Information and Communication

[1] *Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune, India*
[2]*BVCOE, Lavale, Pune*
** Corresponding Author Email: sonali.kothari@sitpune.edu.in*
ORCID - 0000-0002-3797-9932
ORCID -0000-0003-3815-1261
ORDID - 0009-0004-1083-9640

Technologies) have not only impacted the developed countries, rather it has been significantly impacting the developing countries in last two-decades especially in fields like: economics, education, travel and communication [1].

The technology and its importance have been identified as a universal tool of „communication" where it efficiently sorts out the issues like distance, training, career/ business and other aspects. The traditional use of technology has been limited in certain areas (banking, hospital management, film industry, hotel management, travel, etc.) and for certain uses like: data storage, retrieval of data, etc. [2]. Now the technology has been utilized by education sector at its utmost-utility where learning has become creative and innovative. Apart from that, military, healthcare, financial sectors have also been adapting themselves to the technology based environment. Currently, the significant technologies like mobiles, PCs, Laptops and more along with internet has been impacting numerous fields; however where there is positive aspects there would definitely be negative aspects that could affect the development of varied sectors [3].

2. Research Work in Botnet Design and Detection

Mobile botnet is a set of compromised smart phones, which handled through command and control server by Botmaster. The mobile botnets regarded as less endangered of botnet contrast to its counterpart computer based botnet. The evident reason is restrictedpower of battery, limited resources and computation capability, and various medium of communication. This makes smart phones endangered for growth of mobile botnets.

Due to its advanced features, such as those that allow for the storage of bank account information, passwords, net banking information, and information on online payments, mobile devices have been adopted by millions of people. Additionally, the viability of apps that are free on cellphones makes them lucrative targets for thieves and virus programmers.

According to the research of **Oulehla** [4], bot is a special type of malware installed on smart phones. It is a botnet network client acquiring commands from command and control server. On the obtained commands basis bot attempts to carry out malicious performances namely electronic mail spamming, damage of firmware, sensitive information theft, interception of SMS, recording of audio, downloading extra content and click frauds. There are two types of bots. One is hidden bots which comprises of hidden activity which is an app component that offers a screen with which users can communicate to perform something such as taking a photo, dialling a number, viewing amap or sending an electronic mail. A mobile device affected with a bot is known as zombie device. Another type is android app which comprises of illegal part as Fake player while the legal part can carry out some useful work such as playing video or music and illegal part is capable to carry out some criminal tasks.

ccording to the study of **Santos et al.** [5] mobile botnets are powerful and simple methods to establish distributed denial of service attacks that can highly cause reputation of firms and develop their costs of operation. Its huge scale nature and instantly adaptive behavior makes conventional cyber security techniques out-dated. A distributed denial of service attack causes huge number of requests to target server ending its process of legal requests from users. Recognizing imminent botnet targets is essential to assure reliability and resilience of service offered by infrastructure of network.

From the study of **Lu et al.** [6] a mobile botnet can compromise endangered nodes by sending malware through centralized infrastructures. However, to renounce highly developed supervision of mobile infrastructures a furtive way for propagation is to remain off the radar and distribute to endangered nodes nearby which has acquired in existing malware namely Lansco, CPMC and Mabir. It is also stated that mobile botnet have already been predicted in 2009 by Ikbee.B and in 2011 in Android.Binaster. A mobile botnet can be formed in 2 ways namely: 1) infrastructure propagation on mobile markets; and 2) proximity infection.

According to the study of **Karim** [7] the possible attacks of mobile botnets involves propagation of worms and viruses, theft of confidential and private data, generation of spam, unauthorized root access, illegitimate phone calls, control panel access, unauthorized photo and file access, disruption of service referred as distributed denial ofservice attack, outage of power and consumption of memory.

Qi et al. [8] has stated that hackers take benefit of the used loopholes/area of mobile devices to acquire unauthorized access to compromised mobile appliances. The hackers target to carry out unauthorized and malicious activities involving making illegal phone calls, sending electronic mails, using control panel, starting worm code and accessing unauthorized photos or files. **Zhao et al.** [9] has mentioned that Cloud based push styled mobile botnets us a new kind of botnet in mobile surroundings that utilizes push based services of notification to spread the commands. A novel command and control channel is conferred using the C2DM (cloud to device messaging) service which is offered by Google for Android platforms. This channel reveals that Cloud to device messaging is stealthy in terms of power consumption, command traffic, command transformation and bandwidth use to entire bots. Similarly, **Szongott et al.** [10] has mentioned that epidemic malware in mobile is also a new dangerous threat for phone users that disperse quickly in mobile phones. The malware

destroys iOS older versions but it is still an essential treat for smart phone users.

3. Influential Players of Botnet Attacks

The rise of botnet assaults on mobile devices has prompted researchers and analysts to concentrate on the participant elements of mobile botnet attacks since understanding the fundamentals of botnet attacks is crucial for root cause detection and prevention.

Alzahrani and Ghorbani [11] studied about the botnet attacks and their detection techniques and found the core areas of botnet attacks was mainly found through the C&C channel, via C&C communication by the attackers/ hackers. The authors insisted and argued that the huge number of recorded botnet attacks was found through SMS spam which has created a firsthand advantage for the attackers by offering them with better communication and commands over the root node. As per their research, without alerting the network or even the end-user, the attackers can manipulate the C&C commands and take over the information in the end-user‟s mobile phones and then would be sell the information for illegal activities; hence the study states, protecting C&C channel is necessary.

In another research, **Zeng, Hu and Shin** [12] studied about the components and its effects on mobile phone botnet attacks. According to the authors, the main three components would be Vectors (infecting or spreading Bot-codes towards mobiles, especially smart-phones), Channel (for issuing commands) and Topology (in-order to organize an attack via botnet). In their study the authors researched about the various techniques in constructing mobile botnet and as per their findings the process in constructing and infecting mobiles consisted of identifying the components such as vector based propagation, command and control center and also the mobile botnettopology. Thus, authors concluded that without these three basics components constructing and propagating mobiles with botnet is not possible.

Pieterse [13] in his study has researched about the botnet attacks and its process. Similar to Zeng et al., he also argued that the traditional botnet construction and components include three attributes, propagation, channel and topology. He studied in- depth about the components in botnet attacks and insisted that even in non PCs the same three components are required for attacking the user/ mobile phones (smart-phones and androids). According to his research, the OS of mobile phones (Android OS, Windows Phone-7 OS, I-Phone OS, Symbian OS, BlackBerry OS) were compared and assessed for safety and security issues and the number of botnet attacks. As per the findings, the study argues that, protecting OS and communication channels would minimize the botnet attacks in mobiles.

Kundu et al. [14] and **Ahmed et al.** [15] have studied about the mobile botnet attacks and found through their research that the main components in botnet attacks involves communication channel and commands as the source of propagation. In mobiles the botnet attacks could be found through SMS, MMS, E-Mails, Browsing Internet and Downloading files. Although the sources of attacks in mobiles as per the studies states the communication channel as a primary possibility, the in-depth analysis shows that Applications, Spam messages/ Bulk messages: SMS, MMS, E-Mails, visiting the affected sites in internet, Installations of infected Software and Hardware along with Network, etc. could also pave way in affecting mobile phones via botnets.

However **Mantas et al.** [16] studied about the communications and their security. In their study, the authors have found that the security and privacy is the core components of botnet attacks that have been recorded since the last few years. Cybercrimes (eavesdropping, tampering and service attacks), have been identified as most effective attacks in mobile botnet attacks. As per the authors the components the attackers aim at would be the topology, since the attackers seeks information stored by the user. Hence detecting and preventing malicious attacks on mobile phones is quite necessary and essential in the current era.

Thus, it can be assumed from several researchers and their studies that the most significant components of botnet attacks especially in mobile phones comprise of three basic and main factors: **propagation vector, channel and topology**. To highlightdetails about these three factors, following section discusses them one by one. Channelis the C & C server that helps in propagation of botnet using different topologies. Various researchers have highlighted them during research work.

4. Survey On Different Categories Of Botnet Attack

Research work in botnet can be categorized as PC based attack, Mobile based attack andCloud based attack. The section reviews various research work based on these categories.

Midha et al. [17], has stated that criminals spread malicious software referred asmalware that can transform the PC into a bot referred as zombie. When this exists the PC can carry out automated tasks over internet without the user knowing it. Criminals utilize bots to affect huge number of PCs/ These PCs comprise a botnet or network. Criminals utilize botnet attacks to send spam electronic mail messages, attack servers and computers, spread viruses and commit other type of fraud and crime. If the PC becomes a botnet it might be slow and they might be unknowingly supporting criminals. Botnet is feasible in different architectures namely peer to peer, centralized and

hybrid. The hybrid is an integration of centralized and P2P architecture. Botmaster sends commands to the C&C server, which performs operations like P2P and interacts with different commands among themselves. Command and control sends commands todifferent bots under control. Botmaster comprises different F&C centrally. The data mining provides different technologies to retrieve, identity, analyze and discover abnormal and normal patterns. The methods namely are classification, correlation, aggregation techniques, clustering statistical analysis can be used.

According to **Alhomour et al.** [18] botnet is a huge network of compromised PCs anda bot can comprise a network of integrated PCs that are handled by herder or botmaster and utilizes a C&C (command and control) server. Comprised PCs also known as zombies are transformed into a bot. This exists when a user opens or downloads an application of malicious software. The phrase botnet is an integration of two phrases, network and robot so they are also referred robots network. According to **Arabo & Praggono** [19] though computer based botnet is very familiar to cyber community, botnet based on smart device is a new botnet attack that is developing in the cyberworld. Computer based botnets are active for past 2 decades in the world of cyber.Cabir, the first Botent based on Smartphone device emerged in 2004 while Gemini, the first Android bot was invented in China in December 2010. It was a game application with full Trojans. Gemini steals IMEI (International Mobile Equipment Identity) of the affected device, International Mobile Subscriber Identity (IMSI), contact list, coordinates of GPS, details of SMS, etc. and utilized to forward it to the Botmaster.

In [20] **Singh and Chauhan** say that with the emergence of new technologies, life dependence on such portable devices like iPads, smartphones, smart TVs has grown widely. This has established a huge opportunity for cyber criminals to acquire control of user's lives. The internet of things (IoT) and mobile botnets has made their task simpler.Botnet attacks are a well-established and severe threat to online community. These attacks are not only limited to laptops or PCs but also distributing their roots to devices namely refrigerators, medical devices and smart phones. To highlight attacks on deviceslike refrigerators, a router, smart TVs, authors have discussed number of attacks.

5. Propagation of Botnet Using Different Channels

One of the important components in botnet design and detection is the architecture used.The architecture helps in understanding more about botnet. This section highlights someof the botnet attacks with variety of architectures used. To propagate botnet attack, botmaster design C & C server that can employ methods like SMS, MMS, malicious applications, HTTP/s, social networking, email, Bluetooth, NFC etc. for propagation of attack. Here details of botnet attacks categorized using architecture and C & C medium highlighted.

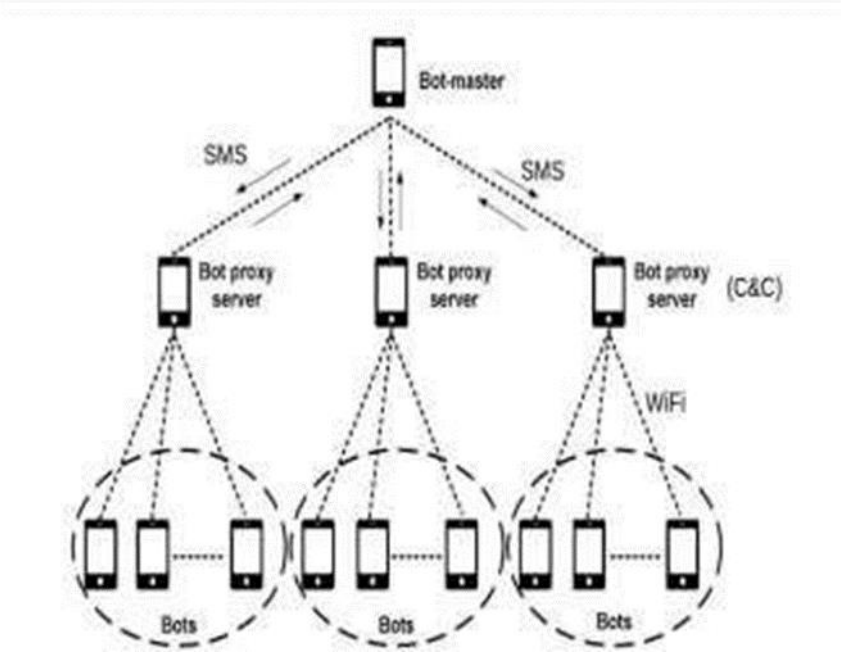

Fig 1: Centralized architecture involving smartphones

Ullah et al. [21] has mentioned that the centralized botnet architecture is simple to control and manage. All affected bots can be controlled and monitored through an individual point. This is the most simple to detect and evolve architecture. SDBot, AgoBot, GTBot, Zotob and SpyBot are some centralized architecture examples. The affected PCs known as bots are often contacting the command and control server in centralized architecture to acquire new requests. A bot master being the network operator sent these requests previously. From the perspective of

botmaster, the command and control servers are the major weak point in the centralized architecture of botnet, in certain cases; a botnet shared amongst numerous bot masters to perform it collectively. It is a common area for hacking the credentials by botnet or taking charge of botnet by another bot master. The bot master can be either a desktop PC or smart phone device that will perform in isolation to avoid detection. The C&C server is a centralized PC or smartphone device that provides commands to zombies on bot master‟s behalf and acquires reports back from them. Relying on the propagation and infection methodologies, botnet can have numerous command and control servers. The phrase originated from the commanding officer of military concept guiding control to her or his forces to achieve a target.

5.1 ATTACKS THROUGH SMS AS C & C

Geng et al. [22] designed an SMS based heterogeneous mobile botnet model. In this study they have revealed how SMS based command and control channel framework can be used by mobile botnets. Author has developed a model made up of bot master, collection node, bot servers, region bot and few bots. Author has divided propagation phase into three steps where first step exploits OS and system vulnerabilities to install bot software. In second step, first tier nodes selected and worked as region bot servers. In third step, nodes start infecting mobile terminals under control of botmaster. The topology used here is P2P structure with SMS and C & C server. Reason about selectionof SMS as C & C is its availability and wide use. Also malicious contents can be easily hidden in SMS message.

Mulliner and Seifert [23] suggested SMS-HTTP C&C system in which the attacker made command and then the command sent to bots through SMS. Then the command uploaded on a designated site in an encrypted file. Every bot decrypt, download the file and send out the commands to other bots through SMS P2P hybrid botnet that utilizes SMS as the C & C channel and P2P network as the underlying framework. Botnet interacts by acquiring commands in a P2P fashion by receiving and sending SMS messages**.**

According to the research of **Hua and Sakurai** [24] as several experienced works are migrated to smart phones they are becoming hot aims of hackers slowly. During the pastfew years, it has seen several malware targeting smart phones and the circumstance is getting bad. Under such situation, a serious query asked whether those affected mobile phones could be organized to a botnet. In this research, the author presents a design of a botnet using SMS as its C&C medium. The author encloses entire perspectives of the botnet design involving the protection of stealthiest, the selection of topology and the maintenance of botnet. The simulations reveals that a newly provided command and control message can be covertly propagated to enclose around 90 percent of the total 20000 bots within twenty minutes based on a simple flooding algorithm. In this method,every bot sends no more than four SMS and the botnet is robust to both selective and random node failures. Thereby, the suggested mobile botnet is a severe threat on mobilecomputing environment security.

5.2 ATTACKS THROUGH BLUETOOTH

As stated in [25], BlueJacking exploits the Bluetooth feature of mobile phone. It is a hacking method to send anonymous messages to other Bluetooth devices in the range. It scans nearby Bluetooth devices, performs handshake and then sends unsolicited messages to the device. In this attacker never has control of other device and so can be avoiding by setting device to disable mode, non-discoverable mode. Other Bluetooth attacks like BlueSnarfing and BlueBugging are actual attacks that may result in user losing its control of the device. BlueSnarfing allows cybercriminals to access victim‟s contact list, emails, calendar and text message when in discoverable mode. In this hackers can respond to queries of other Bluetooth-enabled devices and gaining unauthorized access to information without knowledge of victim. BlueBugging allows hackers to use some features of victim device without user knowledge when device is in discoverable mode. Features of BlueBugging include intercept or reroute communication, send or read text messages, place or monitor phone calls.

Xia W. et al [26] states about Bluetooth based worm Commwarrior targeting Symbian OS. The worm detected in early 2005 used Bluetooth and MMS as method of propagation. It targeted Symbian 60 Series mobile platform with capability of mass mailing random .sis files. In addition to the capability of reproducing through Bluetooth, this malware was the first to utilize MMS (multimedia messaging services) as a replicating mechanism. Propagation methodology used by Commwarrior was very interesting as it uses different time slots for propagating attack. It used Bluetooth for propagation during normal wake hours of user i.e. during 8:00 a.m. to 11:59 p.m. During normal sleeping hours like 12:00 a.m. to 6:59 a.m., it uses MMS to send contact details of infected phones to itself ignoring land line numbers. Besides this, it clears all message logs and MMS details during time frame 7:00 a.m. to 7:59 a.m.

In the study by **Seenivasan and Shanthi** [27], botmaster uses the Bluetooth technique vulnerabilities and make it as the channel of C & C. A Bluetooth based command and control is liable for transmission of command between the Bluetooth enabled devices. It enhances rapid interaction by simplifying the authorization and authentication method. After finishing the process of pairing successfully, a bond will be made between the twoenabled devices of Bluetooth

that develops the building of the C&C channel and makes the devices initiate the interaction. The Bluetooth technique vulnerabilities permit building the stealthy command and control channel that can evade intrusion detection easily and enhance secrecy operation without user‟s knowledge. Bluetooth command and control channel besides the secrecy provide certain extra benefits. Firstly, thebuilding of a Bluetooth command and control will often be feasible because Bluetooth technique is feasible in several devices. Secondly the implementation of the Bluetooth command and control channel is free when contrast to other channels of command and control such as internet or SMS. Lastly, the Bluetooth command and control channel offers cost free and rapid communication of data. These benefits make the Bluetooth command and control channel to avoid detection processes. The Bluetooth commandand control channels have certain weaknesses. Firstly, the gadget must be feasible in close proximity for the building of channel. The communication fails when the devices are out of range. The Bluetooth command and control channel building is feasible when the devices are in near proximity and combined for some time. Secondly, Bluetooth technique consumes more battery power so that the Bluetooth command and control channel assists communication of data for a small period and data transfer is reduced to great extent. If the Bluetooth is left active for an indefinite period, the battery power of the gadget will deplete completely causing the device to shut down and also destruct theBluetooth command and control channel.

5.3 ATTACKS THROUGH ONLINE SOCIAL MEDIUM

Some of the methods employed by social media botnets include [28]:

5.3.1 **Hashtag Hijacking:** It is a real-time marketing practice using which an advertiser uses a popular or trending hashtag to gain visibility on social media [29]. It is like sharp knife, which if used properly can be very useful to get, thejob done but when used carelessly can cause harm and can hurt badly. Twitter hashtag hijacking has faced number of such attacks. It uses Hashtag to target some group or organizations by identifying group-specific hashtags. Botmaster uses the hashtags to spread malicious links that appears in group‟s circle or in news feeds.

5.3.1.1 **Trend-Hijacking or Watering-hole:** This is similar to previous method. In this trending tags were used to directly send link to spread attack to maximum possible number of users. It creates a social watering hole by using trending keyword to harm potential users of the tag.

5.3.1.2 **Spray and Pray:** This type of attacks spreads as many links as possible and prays for at least few visits to the each link. Bots to avoid detection by social media‟s terms of service agreement generate the messages programmatically. The technique is mostly used with one of the above techniques.

5.3.1.3 **Retweet Storm:** In this type of attack, a tweet is reposted or re-tweeted by thousands of other bot accounts resulting in flagging and banning the original posting account though, it does not delete tweets. The parent account in this technique is called as “martyr” as it sacrifices itself for spreading malicious activity.

According to the research **of Al-Dayil and Dahshan** [30] with the rapidly developing mobile networks growth and strong mobile phones, botnets have invaded the domain of mobile or media namely You Tube, Facebook and Twitter have made a new channel of communication for attackers. Presently botmasters initiated to social media for various infected activities namely hiring of new bots, sending spam and control. A detection technique is proposed for mobile botnets based on social media based using Twitter.The suggested method integrates the correlation between user activities and tweeting namely taps or clicks and an artificial immune system detector to predict tweets caused by bots and distinguish them from tweets produced by user or by user-approved applications. The detector creates a tweet signature and contrasts it with a dynamically updated library of signature of bot behavior signatures. The suggested system has been implemented wholly on Android platforms and verified under many generated tweet sets. The test outcomes reveals that the suggested method has a greater accuracy in predicting bot tweets with 95 percent ratio of detection.

According to the research of **Vagheshwari et al.** [31] with the developing growth of internet in mobile and powerful mobile phones botnets have secured the domain of mobile. Social media namely Facebook, YouTube and Twitter have made a new channel of communication for spammers. Bot initiated to use social media for various fake tasks namely hiring of new bots, sending spam and botnet C&C in the suggested system the user sent the tweet on twitter that is recognize that sent tweet sent by bot or user. In suggested model language match that is train according to the language i.e. recognize that sent tweet is generated by human or generated by bot. This study utilizes their own algorithm for recognizing tweet to reduce the messages of spam in social media namely Twitter.

5.4 REAL WORLD BOTNETS DETECTED ON RANGE OF PLATFORMS WITH VARIED C&C CHANNEL

5.4.1 Cabir: Also known as Caribe, SybmOS/Cabir, Symbian/Cabir and EPOC.cabir developed in 2004 was the first computer worm designed to infect mobile phones using Symbian OS and spread as .sis file [32]. Sarwar et al [33] has mentioned that Cabir signaled new era of worms targeting devices with limited computation power like smartphones and PDAs. Worm was capable of infecting non-Symbian phones, PCs and even printers who supports

"Object Push Profile". The worm displayed word "Caribe" every time the phone is turned on and propagated using Bluetooth as C&C medium. It was compatible with mobile phones with ARM series processor like Nokia 60 series phones. Cabir replicated over Bluetooth and stores in message inbox as caribe.sis. Once clicked by user and installed, it searches for nearby Bluetooth devices even mouse or printer and sends malicious file to those devices. Once sent, it disconnects itself from other Bluetooth device thus completing propagation. The steps keeps repeating and propagating attack. However, the worm was not harmful, as it didn‟t do any malicious activity but shortened battery life by continuously scanning Bluetooth devices. KasperKey labs was the first to detect worm by and named it after one of their colleague.

5.4.2 Zeus: It is a malware toolkit allowing cyber criminals to build their own TrojanHorse [34].This is the banking malware having its presence from early 2010 till today. The toolkit is available for sale in black market starting at $3000 where additional modules can cost up to $10000. The malware allows attackers to add new fields in forms to fill out. The website URL seems legitimate but asks user to enter more information related to banking application under the pretext of security. The attack can be propagated as malicious Web links, email attachments and joins as botnet arms once installed on a PC. The Zeus toolkit allows creating number of variants making it difficult to detect by anti-malware software.

5.4.3 IoT based attack: It is first reported attack involving IoT devices discovered by ProofPoint Inc. The attack was occurred during 23 December 2013 to 6 January 2014 [35]. In this attack refrigerator became slave and started sending spam emails to generate DDoS attack. The attacked had infected 100000 devices, which includes televisions, routers, multimedia devices and at least one refrigerator. Infected devices started sending 750000 mails per day in burst of 100000 mails three times a day keeping close look that no more than 10 mails were sent from single IP address to avoid detection. Lack of security to IoT devices is emerged as root cause of such attacks though the devices are available 24*7 online in contrast to PCs. Findings of research team states that attackers have begun to control smart appliances, home routers, and other IoT components to create "thingsbot" network. Use of default passwords made it easily accessible for attackers while consumers are less accessible to virtual device for securing them.

5.4.4 Dendroid: The malware was first discovered in 2014 by Symantec research labs and appeared in the underground for sale at $300. Researchers identified Dendroid as "Remote Access Toolkit" (RAT) targeting Android devices from Western countries and able to breach Google Play‟s security mechanism. Developers claimed that the worm is capable of taking pictures from phone camera, record audio and video, download existing pictures, record calls, send texts etc. Dendroid comes with a universal "binder application" which is a point- and-click capable of injecting Dendroid to innocent user devices.

5.4.5 Necurs: Trend Micro Smart Protection Network detected the malware in February 2014. NECURS and its variants arrive into user‟s system through other malware like UPATRE. It infects device with spammed email attachment or through malicious ads. After infecting device, it disables security services combined with information theft and avoids its detection by deleting malware component files. Some variants of Necurs disable system firewall and does not allow user to turn it on again. This leaves user device vulnerable for other malware attacks.

5.4.6 RottenSys: Swati Khandelwal [36] says that nearly 5 million Android devices released by popular brands were infected with RottenSys malware. The propagation of attack started in September 2016 and earned $ 115000 in just 10 days. It popped aggressive ads, called as impressions in ad industry, 13250756 times in 10 days out of which 478822 were converted in to ad clicks. New smartphones provided by brands like Vivo, Samsung, GIONEE, Honor, Xiomi, Huawei had pre-installed malware "System Wi-Fi service app" and shipped through Tian Pai, a Hangzhou-based mobile phone distributor. Check Point Mobile Security Team who discovered the attack, says that the malware doesn‟t provide any Wi-Fi related service but steals all sensitive Android permission to enable its malicious activities. To avoid detection the malware doesn‟t start infection initially. It receives commands from its C&C about the components required and contains actual malicious codes. It then downloads and installs the malicious code with DOWNLOAD_WITHOUT_NOTIFICATION permission. The malware displays advertisements on home screen, as pop-up windows or full-screen ads to generate fraudulent ad-revenues. As the malware has access to sensitive permissions, it can take full control of millions of devices if received such commands from its C&C. Only option to remove malware is to remove its packages namely com.changmi.launcher, com.system.service.zdsgt, com.android.yellowcalendarz, , com.android.services.securewifi from system.

5.4.7 Star Wars Twitter bot: As per [37], Twitter serves as source of online social media platform with around 328 million active users and 500 million tweets send by users per day. In January 2017, two researchers discovered Star Wars- themed Twitter botnet compromised of 350000 bot accounts known to tweet random quotes from the movie franchise. Though the intention of the attack is still unclear, the botnet can send spam mails, can

create fake trending topics to sway public opinion and launch cyberattack.

5.4.8 WireX: After its introduction in August 2017[2013], this Android bot quickly and successfully attacked tens of thousands of devices. To escape detection and bury itself beneath system operations, the assault carefully awaited its opportunity to unleash itself. The malware was accessible through the Google Play store, but it was taken down once it was discovered. It is now being taken out of affected devices. This "Android Clicker" exploit, which launches a significant application layer DDoS attack, targets Android smartphones running one of the several rogue apps downloaded from the Google Play store. Using 70000 infected devices dispersed across 100 nations, the botnet has infected 44000 Android cellphones. Additionally, more than 300 Google Play store apps have been found to include WireX bot code. The botnet was removed from 300 apps thanks to a partnership of software companies led by Google, including Akamai, FlashPoint, RiskIQ, Team Cymru, CloudFlare, and Oracle Dyn. Most malicious apps with WireX code were downloaded by people in Russia, China, and other Asian nations [38].

5.4.9 Mirai: By 2017, there were 8.4 million linked IoT devices that were either operating with minimal security or even without security. This was exploited by Mirai [39]. According to the paper, Paras Jha, a Rutgers undergrad who is interested in DDoS assaults for financial gain, created Mirai under the code name "Anna-Senpi," which has hardcoded passwords. OVH, a French host, was subjected to the Mirai attack, which started in September 2016. A well-known tool that Minecraft server hosts used to fend off DDoS attacks was hosted by OVH. Attacks against the network and HTTP protocols can both be launched by the attack. After infecting a device, Mirai scans it for further malware before wiping it clean and claiming it as its own. Some Russian-strings were incorporated into Mirai to hint at its creators.

5.4.10 Tizi: According to [40], Tizi is a backdoor piece of malware made specifically to target social media sites. Google Research team discovered it. Tizi was accessible through the Google Play store and was able to bypass Google's Android security measures. Tizi was able to infect 1300 devices before being discovered, primarily in Kenya, Nigeria, and Tanzania. By taking advantage of known weaknesses, Tizi was able to take control of the gadget. According to researchers, Tizi has been around since 2015, and its creator has created websites and social media profiles specifically for deceiving people.

5.4.11 HaoBao: A new and sophisticated crypto currency assault strategy used by the Lazarus cybercrime group was revealed by McAfee Labs [41] to have surfaced in the first quarter. In its first-quarter 2018 threat report, McAffee Labs listed 16 malwares, 23 events, and 25 web and network threats. The cybercrime organization initially launched a recruitment drive for business development executives for a significant global bank with offices in Hong Kong. Users were enticed by the email to download a corrupted Word document from Dropbox. The documents could be opened in the most recent version of Word thanks to a Visual Basic macro that was included in an earlier version of Word. After the user takes this step, malware infiltrates their system and sends data to a command and control server. It functions as a one-time data collection activity that relies on downloading a second propagation state to acquire more access. The term "haobao" is hardcoded into the word document's embedded code, which causes a malicious Visual Basic macro to run. By doing system scans, the obtained data will be used to identify potential targets, particularly those who are using Bitcoin-related applications.

Other than above botnet attacks, following table summarizes few more botnet attacksincluding platforms like mobile phones, PCs, IoT devices with different types of OS

Table 1. Comparison of various botnet attacks

Name of Botnet attack	Architecture/ Methodology used	Findings
RedBrowser	Propagation is through SMS, Bluetooth or through PC. It copies redbrowser.jar file on infected device.	It is a Java Midlet application that runs on J2ME devices. The worm sends SMS to premium rate numbers and causing monetary loss to victim. It shows Red moon picture when application loads. Then displays a message in Russian to trick user and send SMS to some predefined premium rate numbers.
Zitmo	Socially engineered SMS messages are used for initiation and propagation of banking attack.	Zitmo is mobile variant of Zeus designed to attack mobile operating systems like Symbian, Blckberry, Android and Winows. It has targeted specific European users. Purpose of design is to access SMS and mTAN details, to access IMEI,

		IMSI of infected device, perform activities like SMS forwarding, change the C&C phone, mark software for uninstall, clean settings. It is capable of performing illegal transactions. The attack was detected by McAfee research labs.
Plankton	HTTP architecture is used for botnet propagation.	It uses commands like commandstatus, Commands, activate, Bookmarks, history, Installation, Shortcuts, status, Homepage, Terminate, Unexpectedexception for attack propagation. It has the capability to Set Browser Homepage, Get/Set bookmarks, Get/Set list of Shortcuts on the Phone's main Application Page, Send Debugging Info. It has infected more than 2000 devices.
FakeDefend	SMS	It is a ransomware discovered in July 2013 on Android device. It tricks user by performing as antivirus, performs fake scans and display a report of hardcoded infections found on the phone. It asks user to pay for full-subscription. If $99.98 subscription fees is paid through credit card, details of credit card are sent to attacker's server. It deletes some known antivirus application, deletes system files and ROM files, SD card file and locks phone in 6 hours making it unusable.
TigerBot	SMS C&C is used for propagation. It also uses malicious applications for infecting devices.	The attack is designed for infection Android devices. Intention is to gain Financial benefits and Spying/Data stealing. To avoid detection, it uses popular application names and icons, detected by Symantec research lab. It can perform activities like Sending SMS to a pone, Capture Image, Send Network Info., Change APN, Notify of SIM change, Kill specific running applications, Restart the device, report Current Location, Send debug Info.
Chuli	HTTP	Sends contacts list to server, Send Location Info, SMS forwarding, Accessing and Sending Received Calls details. It uses Android commands related to SMS, contacts, location.
Conficker	Uses HTTP pull requests for propagation and comes in various versions.	First variant of the worm was discovered in November 2008. It changes its medium of propagation using advanced malware techniques and forming botnet. The attack is designed to target Windows systems by exploiting flaws in OS and dictionary attacks on administrator passwords to propagate. Approximately 11 million devices are infected and still counting as it releases different versions with different technique.
Android.HeHe	Connect to C&C using Internet connection.	The attack developed for targeting Android device that blocks incoming calls and SMS from some specific numbers. It also steals information from device. The application displays default Android robot icon and fakes as Android security software with package name android.security.component. It needs number of permisisons, updates itself and send stolen information to C&C. The worm is developed in 2014
Linux/IRCTelnet	It affects device operating system and adds into network of bots controlled using IRC C&C.	Written in C++ the botnet was focused on Linux OS based IoT devices by attacking telnet port. It is used to launch DDoS attack with spoofed IPv4 and IPv6 addresses. The attack was written in Italian language and was able to infect 3400 devices. It uses strategy to infect several ports of the network by brute force approach.
SlowBot net	It uses centralized architecture with HTTP/S based C&C server.	The attack is advanced version of Low Obin Ion Cannon (LOIC) attack and capable of performing DoS attack results in shutting down webservers. It performs slow DoS attack in contrast to

		most of the DDoS attacks. The attack has long passive waiting time and short attack time to avoid detection.
Ikee.B	A self-propagated attack which infects jail broken devices without user notification and used to upload user data on its server located in Luthuania. It scans for Netowrk IP addresses and can infect other devices located in different countries.	Designed to infect iPhone with the motivation of revenue generation. It is capable of stealing user device data and self-propagating in nature. The attack was designed for targeted victims within specific geographic region.
AnserverBot	Propagated thru socially engineered SMS messages and trojanised applications.	It uses two layers of C&C server over public blog services with botmaster regularly checking its integrity by verifying signature. It makes backdoor entry to steal private data. The attack was discovered by NetQin research group on Android platform.
Android/Geinimi.A	HTTP with port 8080	Main motivation is to propagate possible malware attack. It steals phone number, IMEI, network operator details, IMSI, voice mail number, SIM operator details, SIM serial number, SIM state, build info. The malware is capable of Send Email & SMS, Make phone calls, Update C&C Address, Selective Deletion of SMS messages, Add new Application Shortcut icons, Create a Bookmark, Display Notifications, List running processes, Perform web search, Display Google Map of current location etc.
Android/PjApps.A	HTTP with port 8118	Uses execmark, execpush, execsoft, exectanc, execxbox commands. Main motivation is to get monetary benefits with propagation to other devices. It steals IMEI, IMSI, phone number,SMS service centre and ICCID details of the infected device. It is capable of inserting bookmark, send SMS, install a new application, open URL in phone browser.
Android/DroidKungFu	HTTP	Motivation is to propagate malware attack. It uses commands execdelete, execinstall, exechomepage, execopenurl, execstartapp, execupbin, execsysinstall. Malware is capable to download, install and execution of other packages, download and install a package in the ”system/app”folder, set browser homepage, open URL in phone browser, download and edit DHCPCD and other files.
Android/Twikabot.A	HTTP	Main motivation is sending SMS to prime numbers to gain financial benefits. It accesses IMEI and contact list. Commands used for propagation of attack includes different type of SMS commands.
Gold Dragon	Initiated through user where socially engineered emails were sent with malicious Word attachment containing PowerShell implant script. The script downloads an image file containing embedded additional Power Shell script in pixels of image.	It can be executed through command line and gathers system-level data of infected system. It profiled the targeted device, gathering information Such as directories on the desktop, recently accessed Files, and program file folder; registry key and value information for the user’s run key. The data is uploaded to its server in encrypted format.

Android/SMS Spy.F	HTTP	Its purpose is of SMS forwarding. If C&C responds with the command (219083), the received SMS message is hide from the user. The intention is to steal SMS and mTAN details.
BankShot	Initiated through phishing email attachment to give remote access of the system to the attacker and enables them to wipe all files.	Designed to target critical infrastructure organizations, financial institutions, health care, telecommunication and entertainment industry. Main motive is to collect data for large-scale future attacks.

6. Characteristics of Android Botnets

With study of various Android based attacks, common characteristics amongst them includes information stealing, messaging, content download, repackaging applications, exploiting permissions.

6.1 **Information Stealing:** Bots does not only download information from C&C but also uploads user information on server. The information uploaded on server includes IMEI, IMSI number, contact list, SMS received, GPS location, Device model etc.

6.2 **Messaging:** Main purpose of such attacks was to earn monetary benefits by sending SMS to premium numbers. However, added feature in Android 4.2 to ask user before sending message to premium numbers, botmaster diverts their action. Messaging now become part of initiating botnet attack and propagating itto further level by luring user with spam SMS and asking to visit and download application from third party market.

6.3 **Content Download:** This type of attacks involves downloading malicious content as an update or luring user to download malicious application from third party stores. Though most of the attacks are initiated from third party stores, it cannot be guaranteed that official play store apps are completely benign. Many such applications are identified on official play store.

6.4 **Repackaged Application:** To work with this attack, botnet owner reverse engineer benign application and upload it with malicious contents. User installs application considering it as benign and fall prey to malicious attack.

6.5 **Exploiting Permissions:** Every application has AndroidManifest.xml file which contains required features and permissions of the application. Some of commonly used features include android.hardware.telephony, android.hardware.wifi, android.hardware.touchscreen, android.hardware.audio, android.hardware.camera while commonly exploited permissions includespermissions related to SMS, contacts and external storage.

7. Case Study of Botnet Attacks with Varied Platform And Methods

This section highlights details about topology and channel employed by various researchers for designing botnet attacks. As various channels are available, proposed research concentrates commonly on SMS, Bluetooth and Social Media as medium of propagation.

7.1 DESIGN OF SPENNYMOOR WEATHER FORECAST APPLICATION TO INVESTIGATE VULNERABILITY OF GOOGLE PLAY STORE:

Milan Oulehla [4] has described vulnerability of Google Play store and available anti-virus software in detecting experimental botnet created during proposed research. The weakness of mobile phone users of ignoring security recommendations over user comfort makes mobile malware propagation easy. Exploitation of Android using proposed research work was not identified by active anti-virus software (AVG Anti- virus, Norton Anti-virus and & Security, Avast Mobile Security and Lookout Security & Anti-virus) installed on infected device.

i. **Design of Pair Applications used for Testing Google Play Security:** [118] has analyzed 1632 Google Play applications with more than million installations each for vulnerability and found that 9.25% (151 applications) analyzed applications have code injection capability. Google Play focuses on dynamic analysis and inspection of AndroidManifest.xml file for identifying suspicious behavior of application like sending or receiving data to and from known C&C servers, multiple requests to same server in a short period of time, which may lead to DDoS attack. A camera application can request READ_SMS,RECORD_AUDIO,INTERNET permissions besides CAMERA permission. Use of such unnecessary permission doesn‟t pose threat for Google Play but can pose threat for user device. Considering these facts, proposed work has designed two applications. First is a testing application, which is a weather forecast application, containing bot controlled by botmaster. Second is the malware application aimed for installing on mobile devices without detected by security mechanism used.

ii. **Working of Created Bot Application:** Weather forecast application contains legitimate and illegitimate code. To work as legitimate app, it shows weather details of Spennymoor town like humidity, temperature, pressure etc. But the illegitimate part of the same application contains JSON data sets having malicious commands. Once the

application is downloaded, bot is automatically launched. JSON dataset containing malicious commands is downloaded as an array of bytes that looks like update of the existing system but is actually a malware application. To launch malicious activities, weatherengine1020 and weather engine support library are used. Being an update, it will not identify by security scans as it works within range of function permission. The proposed research does not steal any information of user devices as it is carried out in controlled environment.

iii. **Characteristics Used to Avoid Detection of Malicious Content:** Though the testing application represents security risk, it was easily published on

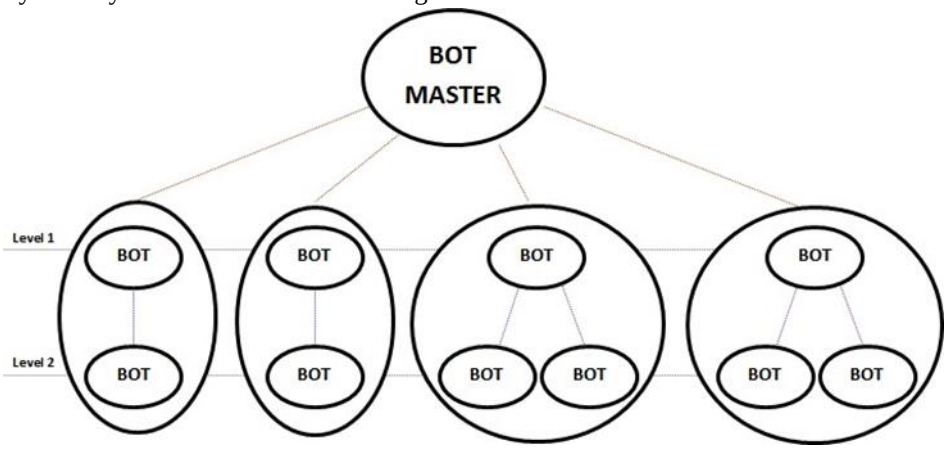

Fig 2: Botnet Propagation Topology using SMS C&C

iv. Google Play store and cannot be identified by Anti-virus software. This has been possible as testing application is carefully designed to minimize possibility of dynamic analysis or analysis of AndroidManifest.xml file. The characteristics are:

1) Testing application does not contradiction between function permission andrequested permission. It performs all its harmful actions using function permission.

2) It doesn't connect to C&C directly. When legitimate weather forecast JSON dataset containing weather forecast information and command for bot is downloaded, then illegitimate malware application starts working.

3) JSON download is initiated by used by clicking update button to update weather details.

4) Bot command is hidden under SHA256 protection provided against manipulation of weather engine making it difficult to identify.

5) Malware application is encrypted as anonymous array of bytes located in

/res/raw directory and escaped from security scans.

6) Cleaning mechanism is performed to remove decrypted installation file from memory of device.

7.2 ANDROID BASED BOTNET WITH ENCRYPTED/DECRYPTED SMS KEYS

Hamandi et al. [43] presented an Android botnet using SMS as channel for propagation. Since all smart phones have services of SMS, author utilizes SMS as the propagation medium of C&C messages between the victim devices and botnet controller.

i. **Botnet attack using SMS Service:** The attack consists of two Android applications, one works as Botmaster while other works as bot. Botmaster maintains list of all infected bots and sends new commands to this bots. Main Activity is the heart of the proposed botnet application. Using this activity, SMS messages are sent and received. Once a new bot joins, it has to send a message and gets itself registered with Botmaster. Botmaster generates a key using 256- bit AES algorithm and sends it to infected device to be used for further propagation. Bot appears to user like benign messaging app used to send and receive SMS to other devices. A listen service is designed to keep track of incoming messages and checks if the message is from one of the infected bots. To maintain track of active bots, bots send "KEEP ALIVE" message from infected device to Botmaster per week allowing Botmaster to tract the infected device mobile number. Communication between Botmaster and bots is carried out using encrypted-decrypted messages and without using any user interface which makes it hard for user to notice any suspicious activity.

ii. **Topology Used:** For designing botnet, centralized architecture is used. Botmaster controls various bots at level 1 of the tree structure which in turn controls bots at level 2. Level 1 bots relays commands to level 2 bots. If bot at level 1 is detected or is removed, level 2 bot replaces it and propagates attacks further [43].

iii. **Required Permissions:** To send and receive SMS, permissions required by application are RECEIVE_SMS and SEND_SMS. Botnet developer has exploited both these permissions. Other permissions related to SMS are READ_SMS and WRITE_SMS which are not used as it is not required. To avoid detection of malicious activity, SMS

payload is encrypted using AES algorithm. To automatically launch infected service after reboot, service is registered as broadcast receiver using BOOT_COMPLETED permission. Once bot is registered with Botmaster, it needs to send a message per week. To avoid sending registration message by bot again and again, Shared Preferences are used.

iv. **Experimentation:** To carry out experimentation work in real life, 3 Samsung smartphones are used where one worked as Botmaster and other two as bots. Encrypted messages were exchanged between them to propagate attacks. VirusTotal uses more than 40 antimalware engines to detect infected applications, IP addresses and/or files. The proposed application was not detected as malicious though it works for stealing user data. Besides this, logcat used to monitor background services was not able to identify infection as propagation is paced at low level. Similarly app was published to download using Android official play store.

7.3 EVALUATING BLUETOOTH AS C&C CHANNEL

According to the research of **Singh et al.** [44] malware targeting smart phones is learntwith developing concern by the community of research. While such attention has focused mainly on worms and viruses most of which utilize near field communication topropagate none have examined whether much complicate malware namely botnets can perform in this surrounding efficiently. In proposed research, author contributed towards development of first characterization of Bluetooth as C&C channel, use of node popularity to create new C&C architecture and developing countermeasures for maximizing command propagation.

i. **Design Methodology:** In proposed research work, Botmaster communicates with very few infected nodes through SMS and cellular data. When infected nodes pass with range of each other, they collect information of other device. Once reached to threshold set by Botmaster, nodes with high degree of connectivity connects Botmaster and provides contact log. This information allows Botmaster to find most likely devices for propagating commands.

ii. **Botnet Architecture:** Following figure shows architecture followed while propagating botnet attack. Darkness around the mobile phone shows its popularity. As phone 0 is most popular, it works as seed for communication with Botmaster. If phone 0 is unavailable, next popular phone connects with Botmaster and report about unavailability of seed node. Botmaster propagates itscommands thru such seed nodes in similar hierarchical structure. Botmaster contacts such seed need in particular area and provides updated payload to be distributed to other malicious bots. These seeds disseminate payloads to large number of devices without them being connected directly to Botmaster.

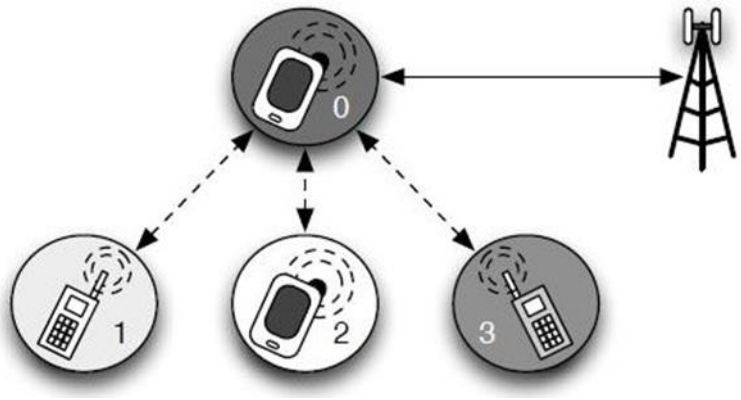

Fig 3: Popularity of Phone to be Selected for C&C

Each bot in the proposed work acts as a peer in the network. Initially bot gets registered using its Universally Unique Identifier (UUID) in the mobile device‟sservice register which makes them discoverable by other bots. When another bot comes in range, a two way Bluetooth connection is established and bot isupdated with latest version of command. The proposed botnet launches denial ofservice (DoS) attack by sending SMS to the devices in its target area. It also simulates Grand Central Station of New York city for its vulnerability forBluetooth based botnet attack.

iii. **Experimental Work:** The proposed research is carried out using Java as development language and simulated on Sun Wireless Toolkit to emulated infected mobile devices. To carry out simulations, trace log datasets provided byMIT under project “Reality Mining Dataset” and “Bluetooth dataset” by NUS were used which helped in evaluation various operational parameters. Forsecond set of experimental work, proposed research has used publically available information for creating simulation model of New York City‟s subwaysystem. It simulates train station and train cars to find out available of infected phone, command transfer rate to support experimental phase.

7.4 TARGETING SOCIAL NETWORKING TO INFECT SMARTPHONES

Faghani and Nguyen [45] proposed a study on botnet design to infect smart phones through online social networking. The suggested botnet is the first that utilizes the online social network platforms as a way to manage mobile bots. The features and structure of online social networks make this botnet difficult to predict, much cost efficient to mobile bots and much resilient to bot failures. Their objective is to raise new mobile botnets awareness that uses online social networks to hire bots so that preventive strategies can be used to deter this type of attack in future. The author also examines the proposed botnet behaviors through simulation to provide a better understanding of this new botnet. Proposed research work uses algorithm proposed by Holme and Beom to create graph with such characteristics to represent OSNs with sizes 5000 nodes, 10000 nodes and 15000 nodes. Three equivalent random graphs (ERG) were generated using above three OSNs using algorithm proposed by Viger and Latapy.

i. **Topology used by Socellbot:** Socellbot exploits two ways of infecting mobile phones, first is to exploit vulnerabilities of the mobile OS and executes the malware code without user intervention. It also sends eye catching web link to user containing malicious code. Using SMS for command propagation may be identified by network provider or by user if it costs huge amount. To avoid detection, each bot in Socellbot forwards command using online social networking messaging system (OSNMS). Initially Botmaster may need to send SMS to few devices for starting infection stage. High clustering capability of OSNs makes working of Socellbot easier. Users tend to create tightly knitgroups by high density of friendships while using OSNs. Due to this characteristic, detection or removal of some bot does not affect working of botnet massively.

ii. **Representation of OSN:** Proposed research represents OSNs as an equivalent graph where each vertex represents a human while links between vertices represents existence of relationship between the human. The proposed research work is carried out using synthesized graphs which possesses all characteristics of real life OSNs. The characteristics includes

   a. If “s” is the vertex and “d” is the degree of vertex in equivalent graph,average network distance of OSN can be given by log (s) / log (d).

   b. OSNs give high local transitivity. That is if X represent a person who isfriend with Y and Z, more likely Y and Z are also friends.

   c. Node degrees of social network graph tend to be power-law distributed.

iii. **Propagation of Malware:** To propagate malware, a node in the OSN is selectedrandomly to work as seed for infiltration. When user executes the commandgiven in malicious web link, infected device sends a message to adjacent vertices in the OSN directing them to malicious code. There is probability “p” that each friend will execute malicious code. Each command to execute malicious content has unique sequence number (SN) and a time-to-live (TTL). Once message carrying malicious contents is received, node checks SN to find ifmessage is already seen before. If its duplicate message it is discarded. If it isnew its TTL is decremented by one and forwards to its one-hop adjacent vertices. In proposed research work, diameter of OSN is used as TTL.

iv. **Simulation Results:** MATLAB is used for simulation of experimentation using discrete-event simulation. Research work is conducted in two sets of experiments. In first set, total number of infected smartphones over time period “T” is measured. It also measures number of newly infected devices over virtual time period “t” which is summarized using $T(t+1) = T(t) + N(t+1)$. Virtual time “t” is defined as the time required by malicious command to traverse one hop in the OSN to reach adjacent vertices of the sender of the command. In second set of experiment, total number of messages sent by infected device via OSN over specific time period is measured. Simulation results of the proposed work shows that ERG is not good choice for Socellbot.

7.5 ADVANCED ANDROID BASED MOBILE BOTNET USING URL FLUX-BASED C&C CHANNEL

Xiang et al. [44] stated about mobile bot that uses flux of uniform resource locator, Andbot is a low cost, resilient and stealthy botnet that employs a botmaster for illegitimate activities in mobile surroundings. This botnet utilizes micro blogs to send malicious commands. Andbot was implemented easily on mobile phones for longer time duration without being detected or noticed. Andbot combines many schemes to make it stealthy and efficient.

i. **URL-flux protocol:** While designing centralized architecture based botnet, Andbot uses URL-flux protocol as C&C channel instead of IRC. In following figure, black circle represents one username, which if blocked or failed to register itself in Microblog, white circle representing another username could be registered making C&C resilient. Andbot connects to one of Web 2.0 servers and tries to connect user with usernames created using Username Generation Algorithm (UGA). If the generated username exists, most recent message will beverified using hard coded public key. If passed, it is confirmed that message is received from authorized botmaster. This type of C&C is termed as “URL Flux” C&C by developers. Conficker attack uses Domain Generation Algorithm

(DGA) and called as “Domain Flux”. In URL Flux, domain purchase is not required and publicly available servers are not required.

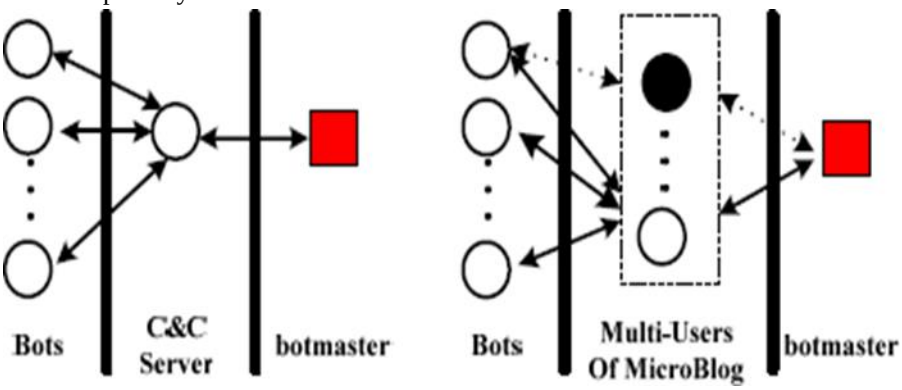

Fig 4: Comparison of IRC Based C&C with URL-flux Based C&C

To avoid detection, other than Bluetooth and SMS, Andbot uses IP only C&C, URL caching, RSS and GZIP compression and sleep command.

ii. **Different Components in Andbot:** As per numbers given in Andbot architecture, various components are explained here. Initially Botmatser encrypts and signs commands and bind cipher text with small JPG image. Botmaster uploads the JPG file to Blog, compresses the URL byrepresenting shorten URL as J1. For next step, Botmaster combines StartDate, ExpireDate and J1 together to encrypt and sign them and then encodes it. The cipher text is published by Botmaster on home page of already registered Microblog user denoted as U2. To start propagation, Andbot keeps visiting Microblog users one by one to find U2. Here UGA algorithm is used for generating usernames. Andbot decrypts J1 based on recent “tweets” of U2, downloads JPG based on J1, recovers plain text commands from JPG and executes commands.

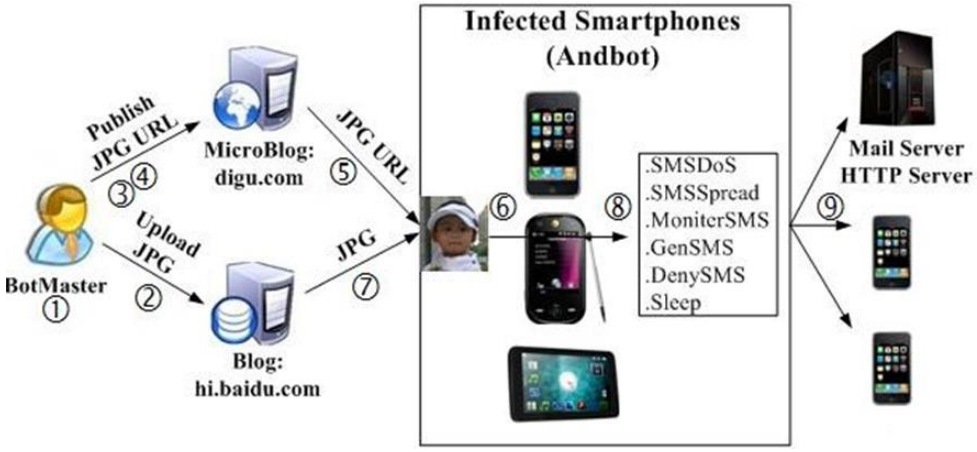

Fig 5: C&C Architecture of Andbot

iii. **Android Supported Commands:** Andbot uses number of commands to propagate its attacking methods. Some of them are explained below

a. .Sleep#Seconds: Allows bot to sleep for some time and avoidresource consumption

b. .SMSSpread#Content#Dest: Sends malicious Content containing phishing message with valid URL to either all contacts in mobile phone of to selected Dest.

c. .MonitorSMS#MobileNumber#Num#Channel#Address: Monitorsnew incoming message or message from special MobileNumber and send it to botmaster via HTTP, SMS or Email determined by Channeland Address

iv. **Experimental Environment:** Andbot uses 4 Android based smartphones HTC Legend with Android 2.2 while Motorola xt502, Motorola xt702 and Samsung i5700 with Android 2.1. WAMP 2.0 was deployed to support Web servic and MySQL database. Web 2.0 Services are used to register with some Micro blogging sites and create accounts. Andbot uses web server and Email to receive stolen information from user devices like IMEI, IMSI, OS version, SMS. Andbot uses famous blog from china “hi.baidu.com” to host JPG files. The experimental work carried out shows that Andbot is low-cost, commands supported, stealthy and resilient botnet attack on Android smartphones.

7.6 EXPLOITING HTTP, BLUETOOTH AND SMS AS C&C FOR HYBRID BOTNET DESIGN

Pieterse and Olivier [46] proposed a study on hybrid command and control channel using SMS and Bluetooth as

propagation medium.. Bluetooth is a familiar technique for short range communication and is used in mobile phones, laptops and tablet PCs. Vulnerabilities related with Bluetooth technique led to developed measures of security enclosing the connections of Bluetooth. Besides the development in security characteristics Bluetooth technique is plagued still by vulnerability use. This study describes the growth of a physical Bluetooth command and control channel, moving beyond earlier studies that much depend on simulations.

i. **Working Methodology Used for Attack Propagation:** In proposed research work, cluster bot works directly receives commands via SMS messages from Botmaster and is responsible for sending those commands to the receiver bot. Receiver bot can be in active state or inactive state. Active receiver participates in dissemination of command while inactive bot executes commands on local device and doesn‟t participate in command dissemination. Botmaster is the entity responsible for sending commands via SMS while mobile bot is theinfected device with two roles either as cluster bot or receiver bot. Mobile bot stores bot list containing IDs of other bots in the specific cluster bot. Command list stores contact numbers of cluster bots to which command needs to be forwarded. Cluster botnet communicates with each other using Bluetooth as C&C channel. Bluetooth MAC address is stored as bot ID. Mobile bots exchange commands using Bluetooth during active period and try to pair with devices available in range during active period only. Once active period isexpired, communication is halted till next active period. Control server is the server managed by Botmaster that stores information about participants of mobile botnet attack.

ii. **Command Dissemination:** Specific predefined activities are available with all mobile bots to disseminated commands. The activities can be static activity or dynamic activity. Static activity occurs only once during initial infection of mobile device. In static activity, mobile phone number and Bluetooth MAC address is collected. During dynamic activity which occurs regularly during lifetime of botnet, location data during active period is collected. It also verifies if control server is still active. During low mobility period, the information is forwarded to control server by inactive infected bot device. To communicate with control server, HTTP C&C is used as communication channel. Once forwarded, it waits for active period and becomes active. At its active stage, it receives commands from cluster bot and disseminates to other devices. The purpose of the botnet attack is to gather location data of the infected devices along with collecting IMEI, IMSI and contact numbers stored on infected devices.

iii. **Experimental Setup:** Proposed prototype is designed using small collection of mobile phones having Android OS. The devices used include Samsung Galaxy Pocket, Samsung Galaxy S2 and Google Nexus Tablet 7. The malicious code is developer for version 2.3.3 or higher. The experimentation carried out using the setup shows that the botnet prototype proposed here achieves required characteristics: no single point of failure within hybrid topology, low monetary cost for command dissemination, low battery consumption per bot and limited network activities.

7.7 HONEYPOT DETECTION BY BOTMASTER IN ADVANCED BOTNET ATTACK

Ping Wang et al. [47] have proposed detection of honeypots in advanced botnet attacks. Botnet defenders have limitation that they cannot allow their honeypots to participate in real botnet attack that can be harmful to others while cyber criminals do not have any such restriction which makes their work easier than defenders.

i. **Detection of Honeypot Bots:** Proposed method depicted in following figure detects honeypots that are infected and acting as bots in botnet In this technique, an infected computer sends malicious traffic to one or several remote computers actually controlled by botmaster. These remote computers work as botnet sensors. If it receives complete traffic from infected host, it is considered as normal bot and not the honeypot. IP address of such bot is informed to C&C server who authorizes the bot to join botnet The botmaster uploads authorizationkey to the host allowing it to join botnet but only when host passes honeypot detection test. Botmaster may perform honeypot test periodically when authorization or encryption key is changed or when bot software is updated.

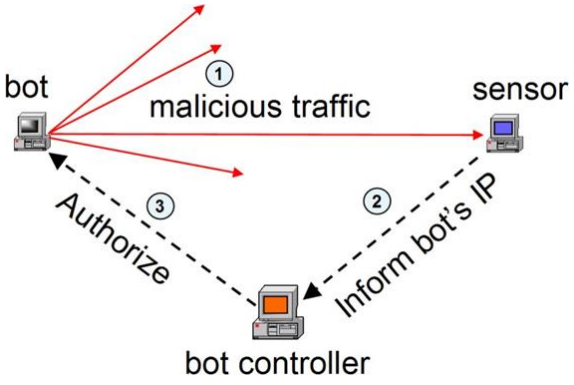

Fig 6: Detection of Honeypot Bot in Hierarchical Architecture

ii. **Detecting Honeypot Through Infection:** Honeypots like GenII honeynets employ Network Intrusion Prevention System (NIPS) that can modify malicious traffic to disable malicious activity. Botmaster need to verify that traffic sent by bots is not altered. To avoid detection of sensor‟s identity, bot stores IP address of sensors at random point in the list of IP addresses to be scanned. To avoid detection of bot, which infects using email attachment, sensor‟s email address is kept at random location in senders list. This will delay newly infected bots participation in botnet but the delay is affordable to botmaster. Honeypot defenders need to perform binary code analysis to detect sensors IP address that can be made more difficult by botmaster by encrypting IP address in the code.

7.8 EXPLOITING C2DM SERVICE FOR CLOUD-BASED BOTNET

Google‟s Cloud-to-Device-Messaging service (C2DM) is a mobile notification service that allows developers of Android applications to send data from servers to their applications and Chrome extensions. **Shuang Zhao et al.** [48] have proposed botnet attack to exploit this service for developing cloud-based mobile botnet attack. Authors also suggested to monitor AndroidManifest.xml file of the application for entries of "com.google.android.c2dm.permission.RECEIVE" permission. More entries of this permission can be warning of malicious activity.

i. **Push Notification Service:** Many of the popular smartphone platforms provide push notification service to send data to mobile applications. The service is comprised of a cloud with capability of push-based messaging servers that are responsible for forwarding messages from application servers to mobile applications. Application server sends notification message a cloud-based messaging server that pushes the message to targeted receiver or mobile device. This service removes need of mobile devices to visit application servers periodically for messages while application servers do not need to keep track of status (active or inactive) of mobile device thus reducing payload of application servers. Other than C2DM service, some known push notification includes Blackberry‟s Push service (BPS), Microsoft‟s Push Notification Service (MPNS) for Windows phones, Apple‟s Push Notification Service (APNS) for iOS, Nokia‟s Notification API (NNA) for Symbian and Meego.

ii. **C2DM Working:** To understand working of C2DM botnet, the proposed method first discusses working flow of C2DM method in following diagram. To use C2DM service, mobile must have logged-in to at least one Google account.

a. To use C2DM service application developer needs to sign up of account with C2DM server by providing C2DM username, password and package name of the mobile application. After establishing account, developer can embed application with C2DM username and publish it through official play stores or third party markets.

b. When mobile application is first launched in mobile device, it registers itself with one of the C2DM servers with C2DM username available with application and device ID to uniquely identify device hosting the application.

c. C2DM server provides a string of bytes as unique registration ID to allow server to identify application running on a specific Android device.

Fig 7: Workflow of C2DM

d. The mobile application sends the registration ID and username to application server which will get stored in database.

e. To send data to mobile device, application server

needs authorization token from C2DM server. For this, application server sends C2DM username and password for verification. To send notification message to "n" number of devices, application server sends "n" number of notification requests to C2DM server with authorization token, registration ID of application and notification message.

f. Using registration ID in request, C2DM server sends notification to the application on specific mobile device (if connection C2DM connection of the device is active). If mobile device is disconnected then the notification message will be stored by C2DM server and will be forwarded when connection with mobile device will be established.

iii. **C2DM Botnet Architecture:** To propagate botnet attack using C2DM service, botmaster needs to establish account with C2DM server as explained in previous step. After establishing account, botmaster can follow below steps when a new bot joins the botnet

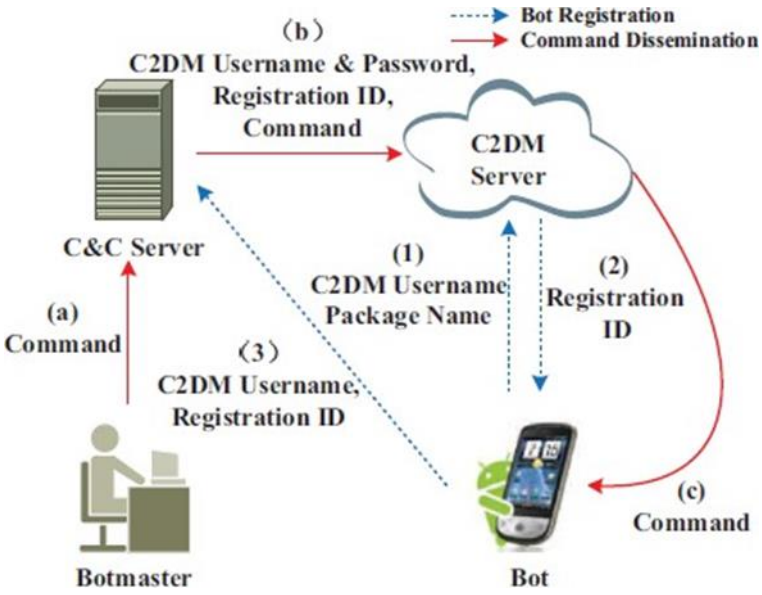

Fig 8: Working of Basic C2DM Botnet Rrchitecture

1) Botmaster embeds C2DM user name and packager name in distributed malware package. When a new device registers itself with C2DM server using this details along with its Google Account knowingly or unknowingly, it joins botnet If the registration is successful, C2DM server assigns registration ID to the infected device. The newly joined bot forwards C2DM username and registration ID to C&C server, which in turn will be stored by botmaster in its database.

2) To propagate commands to infected devices, botmaster asks C2DM server for authorization token by providing its C2DM username and password. On receiving token, botmaster sends notification request to C2DM server with notification message that will work as bot command, registration ID and authorization token. Using registration ID, C2DM server will push the message to bots

3) To enhance this attack, botmaster can use two different C2DM user names, one for itself to work as legitimate application and other by its bot tocommunicate with C&C server.

4) To upscale attack at large level, authors have suggested creation of small networks of bots with number of C2DM accounts and a unique username to communicate amongst them and with botmaster.

iv. **Experimental Results:** As proposed by authors, Google allows same package name to be used by different users while registering to C2DM service. If a common social networking like Facebook, Twitter package name is used by botmaster, Google will not ban it as it may affect other legitimate service. To register with C2DM server, username must be unique. To avoid botnet propagation, Google can ban malicious or suspicious username. This can be avoided by using more than one account to register with C2DM server. During experimentation, authors have studied botnet attack for stealthiness by traffic, commands or data transfer. The authors observed that none of them are detected as their botnet produces much lesser traffic than the legitimate applications avoiding detection. It is also observed than bandwidth consumption of C2DM botnet is much lesser than that of IRC and HTTP based botnet attack. Besides this power consumption of C2DM botnet is much less than HTTP bot and is equivalent to IRC bot.

8 Conclusion

Mobile botnet can lift the data from smart phones without user‟s knowledge. In present circumstance it is simple to attack smart phones than computer based network. The

reason lies in lack of knowledge about the risks and threats by end users, mobile network operator‟s negligence in offering security to their customers and inadequate efforts by application providers and developers in offering security against malware detection and development.

The literature review chapter highlights some of the common botnet attacks based on different platforms from PCs, cloud, mobile phone IoT devices etc. The chapter completely explores the field of mobile botnet attack through discussion of various existing mobile botnet attack. Each system is explained using an approach used to design botnet attack with different C&C channel which includes design methodology, dataset used, architecture, experimental setup and results.

References

[1] M.O. Ogbomo and E. F. Ogbomo, "importance of information and communication technologies (icts) in making a healthy information society: a case study of ethiope east local government area of Delta state, Nigeria", Journal on Library Philosophy and Practice, pp. 1-8, 2010.

[2] K. Courville, "Technology and its use in education: present roles and future prospects", 2011 Recovery School District Technology Summit, Current Trends and Recommendations in Technology, Baton Rouge, Louisiana, pp. 1-19, 2011.

[3] L. Stosic, "The Importance of Educational Technology In Teaching", International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE), vol. 3, no.1, pp. 111-114, 2015.

[4] Milan Oulehla, "Investigation into Google Play security mechanisms via experimental botnet", 2015 IEEE International Symposium Signal Processing and Information Technology (ISSPIT), Abu Dhabi, United Arab Emirates, pp. 591-596, December 2015.

[5] Augusto Almeida Santos, Michele Nogueira, José M. F. Moura, "A stochastic adaptive model to explore mobile botnet dynamics", IEEE Communications Letters, vol. 21, no. 4, pp.753-756, December 2016.

[6] Lu, Z., Wang, W., & Wang, C, "On the evolution and impact of mobile botnets in wireless networks", IEEE Transactions on Mobile Computing, vol. 15, no. 9, pp.2304-2316, 2016.

[7] Ahmad Karim, Syed Adeel Ali Shah, Rosli Salleh, Muhammad Arif, Rafidah Md. Noor, Shahaboddin Shamshirband, "Mobile botnet attacks – an emerging threat: classification, review and open issues", KSII Transactions on Internet and Information Systems, vol. 9, no. 4, pp.1471-1488, March 2015.

[8] Qi, H., Shiraz M, Gani A, Whaiduzzaman M and Khan S, "Sierpinski triangle based data center architecture in cloud computing", The Journal of Supercomputing, pp. 1-21, 2014.

[9] Shuang Zhao, Patrick P. C. Lee, John C.s. Lui, Xiaohong Guan, Xiaobo Ma, Jing Tao,"Cloud-based push-styled mobile botnets: a case study of exploiting the cloud to device messaging service," Proceedings of the 28th Annual Computer Security Applications Conference, December 2012.

[10] Christian Szongott, Benjamin Henne, Matthew Smith, "Evaluating the threat of epidemic mobile malware," 2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, December 2012.

[11] Abdullah J. Alzahrani and Ali A. Ghorbani, "SMS-based mobile botnet detection framework using intelligent agents", Journal of Cyber Security and Mobility, vol. 5, no. 2, pp.47-74, January 2017.

[12] Yuanyuan Zeng, Xin Hu, Kang G. Shin, "How to Construct a Mobile Botnet?", Article on Mobile Phones, pp. 1-2, 2010.

[13] H. Pieterse, "Design of a hybrid command and control mobile botnet", PhD. Thesis, Computer Science, University of Pretoria, July 2014.

[14] Ashish Kundu, Zhiqiang Lin, Joshua Hammond, "Energy attacks on mobile devices", ACM Journal, vol. 1, pp. 1-11, April 2017.

[15] Rizwan Ahmed and Rajiv R. Dharasakar, "Study of mobile botnets: an analysis from the perspective of efficient generalized forensics framework for mobile devices", National Conference on Innovative Paradigms in Engineering & Technology (NCIPET-2012), pp. 5-8, March 2012.

[16] Georgios Mantas, Nikos Komninos, Jonathan Rodriguez, Evariste Logota, Hugo Marques, "Security for 5G Communications", in Fundamentals of 5G Mobile Networks, John Wiley & Sons Ltd, pp. 207-220, May 2015.

[17] Kalpna Midha, Kusum Rajawat, Vijay Singh Rathore, "An introduction to botnet attacks and it's solutions", International Journal of Computer Applications and Information Technology, vol. 1, issue 2, pp. 37-41, September 2012.

[18] Adeeb Alhomoud, Irfan Awan, Jules Pagna Disso, "Towards an enterprise self-healing system against botnets attacks", 2013 International Conference on Computing, Networking and Communications (ICNC), San Diego, CA, USA, January 2013.

[19] 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, September 2013.

[20] Jai Puneet Singh, Akashdeep Chauhan, "Detection and prevention of non-PC botnets". [Online]. Available: http://vixra.org/pdf/1709.0402v1.pdf [Accessed August 17, 2023].

[21] Ihsan Ullah, Naveed Khan and Hatim A. Aboalsamh, "Survey on botnet: its architecture, detection, prevention and mitigation", IEEE Transactions, pp. 660 -665, 2013.

[22] Guining Geng, Guoai Xu, Miao Zhang and Yanhui Guo, Guang Yang, Wei Cui, "The Design of SMS Based Heterogeneous Mobile Botnet", Journal of Computers, vol. 7, issue 1, pp. 235-243, 2012.

[23] Collin Mulliner, Jean-Pierre Seifert, "Rise of the iBots: Owning a telco network", 2010 5th International Conference on Malicious and Unwanted Software, IEEE conferences, Nancy, Lorraine, France, pp. 71-80, October 2010.

[24] Jingyu Hua and Kouichi Sakurai, "A SMS-based mobile botnet using flooding algorithm", WISTP 2011: Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication, Springer, Berlin, Heidelberg, pp. 264-279, 2011.

[25] "BlueJackig, BlueSnarfing and BlueBugging", Techopedia. [Online]. Available: https://www.techopedia.com/definition/5046/ [Accessed 24 August 2023].

[26] W. Xia, Z Li, Z Chen and Z Yuan, "Commwarrior worm propagation model for smart phone networks", The Journal of China Universities of Posts and Telecommunications, vol. 15, no. 2, pp. 60-66, 2008.

[27] D. Seenivasan and K. Shanthi, "Categories of botnet: A survey", International Journal of Computer and Systems Engineering, vol. 8, no.9, pp.1689-1692, 2014.

[28] Payal Chandak, H. P. Channe, "Design and detection of social media botnets using event-driven analysis", International Journal of Innovative Research in Computer and Communication Engineering, vol. 5, issue 5, pp.10094-10097, May 2017.

[29] "Hashtag hijacking: the good, the bad, and the ugly", AgencySparks, November 10, 2016. [Online]. Available: https://www.agencysparks.com/blog/hashtag-hijacking [Accessed August 24, 2023]

[30] Reham A. Al-Dayil, & Mostafa H. Dahshan, "Detecting social media mobile botnets using user activity correlation and artificial immune system", 2016 7th International Conference on Information and Communication Systems (ICICS), IEEE Conference, Irbid, Jordan pp. 109-114, April 2016.

[31] J. Vagheshwari and S. Swarndeep, "Detecting bot messages from social media using language match algorithm", International Journal of Advance Research and Innovation Ideas in Education (IJARIIE), vol. 3, issue 2, 2017.

[32] "Bluetooth-Worm:SymbOS/Cabir", FSecure [Online]. Available: https://www.f-secure.com/v-descs/cabir.shtml [Accessed: June 14, 2023]

[33] Usman Sarwar, Sureswaran Ramadass, Rahmat Budiarto, "A framework for detecting Bluetooth mobile worms", 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, Penang, Malaysia, pp.343-347, May 2007.

[34] "Zeus Trojan (Zbot)", TechTarget SearchSecurity, May 2012. [Online]. Available: https://searchsecurity.techtarget.com/definition/Zeus-Trojan-Zbot [Accessed June 14,2023]

[35] "Proofpoint Uncovers Internet of Things (IoT) Cyberattack", Proofpoint, January 16, 2014. [Online]. Available: https://www.proofpoint.com/us/proofpoint-uncovers-internet-things-iot-cyberattack [Accessed June 14, 2023]

[36] Swati Khandelwal, "Pre-installed malware found on 5 million popular Android phones", The Hacker News, March 15, 2015. [Online]. Available: https://thehackernews.com/2018/03/android-botnet-malware.html [Accessed June 14, 2023]

[37] "Top 5 botnets of 2017", PentaSecurity, December 22, 2017. [Online]. Available: https://www.pentasecurity.com/blog/top-5-botnets-2017/ [Accessed June 14, 2023]

[38] Mohit Kumar, "WireX DDoS botnet: an army of thousands of hacked Android smartphones", The Hacker News, August 28, 2017. [Online]. Available: https://thehackernews.com/2017/08/android-ddos-botnet.html [Accessed June 06, 2023]

[39] Josh Fruhlinger, "The Mirai botnet explained: how teen scammers and CCTV cameras almost brought down the internet", CSO from IDG March 9, 2018. [Online]. Available: https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html [Accessed June 14, 2023]

[40] Brandon Vigliarolo, "Google stops the spread of Tizi Android malware in the Play Store", TechRepublic, November 28, 2017. [Online]. Available: https://www. techrepublic.com/article/google-stops-the-spread-of-tizi-android-malware-in-the-play-store/ [Accessed June 14, 2023]

[41] McAfee Labs Threats Report, June 2018, [Online]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2018.pdf [Accessed June 14, 2023]

[42] Milan Oulehla, "Investigation into Google Play security mechanisms via experimental botnet", 2015 IEEE International Symposium Signal Processing and Information Technology (ISSPIT), Abu Dhabi, United Arab Emirates, pp. 591-596, December 2015.

[43] Khodor Hamandi,Imad H. Elhajj, Ali Chehab, Ayman Kayssi, “Android SMS botnet: A new perspective”, 10th ACM International Symposium on Mobility Management and Wireless Access, pp. 1-6, October 2012.

[44] Kapil Singh, Samrit Sangal, Nehil Jain, Patrick Traynor and Wenke Lee, “Evaluating Bluetooth as a medium for botnet command and control”, DIMVA 2010: Detection of Intrusions and Malware, and Vulnerability Assessment, Springer–Verlog, Berlin, Heidelberg, pp. 61-80, 2010.

[45] Mohammad Reza Faghani, Uyen Trang Nguyen, “Socellbot: A new botnet design to infect smartphones via online social networking”, 2012 25th IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), Montreal, QC, Canada, pp. 1-5, May 2012.

[46] Heloise Pieterse and Martin S. Olivier, “Bluetooth command and control channel”, Computers & Security, pp. 75-83, May 2014.

[47] Ping Wang, Lei Wu, Ryan Cunningham, Cliff C. Zou, “Honeypot detection in advanced botnet attacks”, International Journal on Information and Computer Security, Inderscience Enterprises Ltd., vol. 4, issue 1, pp. 30-51, January 2010.

[48] Shuang Zhao, Patrick P.C. Lee, John C.S. Lui, Xiaohong Guan, Xiaobo Ma, Jing Tao, “Cloud-based push-styled mobile botnets: A case study of exploiting the cloud to device messaging service”, ACSAC '12 Proceedings of the 28th Annual Computer Security Applications Conference, Orlando, Florida, USA, pp. 119 – 128, December 2012.