ABSTRACT—As most applications in wired networks become available on mobile devices and mobile networks are well integrated with Internet, Botnet becomes the most crucial threat to mobile devices, but they are still rare for the mobile world. It's become the considerable threat to cyber security and also used as an infrastructure to carry out nearly each type of cyber-attack. We have studied a new hybrid scheme for the prevention of a mobile botnet for VPN. We have studied the various Mobile Threats, Detection of Mobile Botnet for VPN i.e. virtual private network is digital network-based security technology and security requirements of mobile smartphone.

Index Terms—Virtual Private Network; Botnets; Cyber Attacks;

1. INTRODUCTION

VPN is a virtual private network. VPN, in the modern sense, is generally considered to be a digital network-based security technology. However, in the past, the understanding of VPN is using a dedicated communication line to build dedicated remote connection service. In order to contact the staff of different locations, many large enterprises spent expensive money hiring lines, such as telephone lines, Frame Relay, ISDN or ATM network. With the growing popularity of the Internet, people began to try to structure their own private network on the Internet. But the first problem waiting to be solved is safety, because the Internet itself is open and cannot provide any security [10].

A virtual private network has the provisioning of private network services for an organization or organizations on a public or common infrastructure such as the Internet service provider backbone network. The shared service provider backbone network is named as the VPN backbone and is used to transfer traffic congestion for many VPNs, as well as non-VPN traffic. A virtual private network (VPN) provides a secure connection between a sender and a receiver over a public non-secure network such as the Internet. A secure connection is generally associated with private networks. Using the techniques discussed later in this chapter, a VPN can change the characteristics of a public non-secure network into those of a private network.

VPNs reduce remote access costs by using public network resources. Compared to other solutions, including private networks, a VPN is inexpensive. The goal of a VPN is to provide a secure passage for users’ data over the non-secure Internet.

Figure 1.1: Network Model of VPN

It enables companies to use the Internet as the virtual backbone for their corporate networks by allowing them to create secure virtual links between their corporate office and branch or remote offices via the Internet. The cost benefits of VPN service have prompted corporations to move more of their data from private WANs to Internet-based VPNs.

1.1. Types of VPN

Currently there are three types of VPNs. While their goal is to leverage the Internet as a private enterprise...
backbone network, each of them addresses the needs of a different interest group in the enterprise. The three types of VPNs are as follows:

1. Access VPNs provide remote users such as road warriors (or mobile users), telecommuters, and branch offices with reliable access to corporate networks.
2. Intranet VPNs allow branch offices to be linked to corporate headquarters in a secure manner.
3. Extranet VPNs allow customers, suppliers, and partners to access corporate intranet in a secure manner. Because of their growing importance in corporate networking.

2. BOTNETS

Botnets are the most dangerous security threats to the Internet and the desktop computer world, but they are still rare for the mobile world. Recently, with the rapidly-growing popularity of smartphones, such as the iPhone and Android-based phones, attacks on cellular networks and devices have grown in huge number. Mobile systems are now days are using Internet connection through High-Speed Downlink Packet Access, Universal Mobile Telecommunication System, Enhanced Data Rates for GSM Evolution (EDGE) and General Packet Radio Service (GPRS) which are not same IP based technologies evolved within the mobile network and wireless network [1]. The very next upcoming generation of networks will be mobile broadband where the mobile device will remain online and connected to the Internet all the time. Mobile terminals are becoming more and more like desktop computers. Several studies on Botnets and mobile devices predict transferring data on the Internet.

The connection between the traditional Internet and the mobile network may act as a gateway for malware to move between these networks. Infection vectors are used to spread Internet malware are extended using SMS, MMS, Bluetooth and synchronizing between the computer and the mobile peripherals. Malware on mobile devices can move using infections vectors on the Internet as email, web pages and social engineering. What advantages can be gained using mobile device as a botclient? Are there any economic profits, is there any unwanted action to do through the mobile network? Can mobile Botnet become as tough to visit and close down as Botnets on the Internet? By having a botclients on mobile devices a botherder will be able to destroy the services in the mobile network. By nature mobile devices will not be available on the Internet all the time. They switch between available communications channels on the Internet or on the mobile network [7].

2.1. Detection of Mobile Botnet

[12] In trying to keep pace with Botnets, defenders have constantly tried to mitigate the harmful intentions of Botnets by coming up with novel solutions, targeted at the core architectural footprint of Botnets. Some of the solutions use static analysis techniques via reverse engineering the bot binaries using programs such as IDA pro or perleyez. Other approaches have used a dynamic analysis approach using tools such as cw sandbox or norman sandbox by performing windows API hooking; or performing system wide dynamic taint tracking.

Botnet emulation approaches testbeds such as EMUlab/ DETER/ WAIL have also been used to emulate an entire Botnet by setting up command-and-control servers, infected clients and local DNS resolvers.

2.2. Approaches to detect mobile Botnet

2.2.1. Botnet detection using honeypots

The methodology to detect and penetrate Botnets in the past years has been done with the use of honeypots. A honeypot can be loosely defined to be a machine that is closely monitored to watch for potential infiltration. The honeypot is a machine that running on the virtual environment but looks like a real vulnerable machine. The use of honeypots lies in the fact that any traffic that tries to contact a honeypot can be considered as inherently malicious since by default, honeypots do not by themselves contact other hosts unless instructed to do so and hence should not exhibit any network traffic. The use of more than one honeypot in a network is called a honeynet.

2.2.2. Spamming Botnet detection

The primary utility of Botnets is in sending spam, many researchers have looked into analyzing Botnets that are used exclusively for sending spam such as the Storm, Srizbi and Rustock Botnets. Though the size of spamming Botnets has reduced significantly due to internet service providers blocking Command & Control Servers as well as the domain providers for these Botnets, spamming Botnets remain an active Threat. Used a DNS blacklisting technique (DNSBL) where it creates a graph of nodes that are
in any way linked to the known srizbi Botnet. If a bot belonging to srizbiqueries a large DNSBL of an internet service provider, correlation of the querying node or the one being queried with the srizbi list gives a list of new peers who are infected by srizbi. This process could be repeated multiple rounds to find out all associated bots which send spam [12].

2.2.3. Network-based Botnet detection
Some Botnet detection systems have relied on detecting bot traffic using network level data. This is mainly done using network sniffing intrusion detection tools such as snort in addition to other network flow monitors.

2.2.4. Behavior analysis based Botnet detection
More recently, researchers have attempted to detect Botnets by tracking their network and host behavior. [12] Recently proposed the correlation of behavior analysis of malware via clustering of behavior of host system calls via their ANUBIS dynamic analysis tool and the use of Locality Sensitive Hashing (LSH) clustering algorithm. Their tool works by performing an offline analysis of a malware sample similar to CWSandBox. The authors mention that capturing behavior at a system call level causes data explosion and increased false positives and negatives if an adversary has the knowledge that a system is tracked at a system call level.

3. RELATED WORK

In the paper [2] has proposed a mobile Botnet detection method that detects “pull” style C&C medium how, where, when to detect botnet. Their network based scheme detects Botnet by inspecting flow features of C&C traveling through VPN which provides a shared path for both third and fourth generation and Wi-Fi. Through the verification analysis under real Botnet attacks, they have proposed scheme that provides very high detection rate by using unwanted models as well as very low FP rate by adding on whitelist or signatures.

In the paper [8] the basic detail of Botnets characteristics along with their malicious activities is given and also give a review of advantages and disadvantages of the Botnet detection techniques. Recently, Botnets have become the largest threat for cyber security and have been used as an infrastructure to carryout nearly each type of internet onset. Bots are dynamic of nature and the Botmasters, who control them, update the bots and transform their codes from day to day to control the current detecting techniques. Due to day to day updating and change in nature, Bots are very difficult to detect. [8] Discuss current challenges and give suggestion for the future work according to their behavior, lifecycle, nature.

In the paper [9] present an overview of upcoming generation of mobile botnet named as MoBotstudies on the new command and control mechanisms, actual instances and malicious activities and review the current challenges and limitations of Botnet detectionin mobile environments. Mobile devices are now well integrated with the Internet and amount of mobile device increase day by day very rapidly. Due to this rapid increase of mobile devices on internet, there security become a critical issue. Mobile user pay very less attention towards the mobile security as compared to Computer user proposing new structure and communication model instead of detecting or responding to Botnets.

In the paper [10] propose a Botnet named as SocellBotthat uses the Online Social Network means to avoid cellular bots. The structure and features of OSNs make this Botnetharder to get detected, more resilient to bot failures and more cost effective to cellular bots. Their objective is to raise the awareness of new mobile Botnets that will destroy OSNs to hire new bots so that prevention measures can be implemented to deter this type of danger in the future. They also analyze the behaviors of the proposed Botnet via simulation to offer much better understanding of the latest type of Botnetworks.

In the paper [1] analyses the different attacks on the mobile that are done by a Botmasters using Zombie machine called as Botnets. Botnet is a critical security threat on the Internet. Botmaster who control the Botnets, day by day develop new infrastructure and techniques to scoff security investigators. In past years, the amount of mobile devices were less that connected to internet, so the security of mobile from Botnets not a big issue. But now time change, Mobile Networks are well integrated to the internet, so that threats on the Internet most likely will migrate over to the mobile networks and vice versa. Botnets attacks very rapidly on mobile and show their existing very quickly.

In the paper [4] all others viruses, worms, trojan horse are the very famous and familiar threats on the internet but apart from these there is a less familiar and exponentially growing threat that tends to be
more catastrophic called as Botnet. Botnet target on the integrity and resources of users that might be teenagers evidencing their hacking skills to organized criminal syndicates, disabling the infrastructure and causing financial damage to organizations and governments. It is crucial to know in what ways the system could be targeted. In this paper IRC, HTTP, P2P are the three types of Botnet on the basis of attacking techniques. By using one of these Botnet attack on mobile. The major advantage of this classification is to identify the problem and find the specific ways of defense and recovery.

In this paper[5] presented an attacker-centric paradigms of threats for mobile technology to analyze attacker's objectives, attack vectors. Unauthorized goals is defining the motives for attacking mobile platforms in order to identify the attacker's interests and potential aims. Attack vector defines as the model incorporates the attack vectors in order to present possible entry points for malware content on mobile devices. Mobile devices are fastly becoming tempting targets for attacks due to significant advances in both hardware and operating systems (OS). Attacks on mobile device also increase as on PCs. With the help of internet, the mobile device works as same of computer so infection by Botnets increases. So needs to develop a system that attract the Bots and identify behave and nature.

In the paper [6] propose an approach that uses network-based problem detection to find out Botnet C&C Channels in a local network that does not include any prior knowledge of signatures or C&C Server addresses. This detection method can detect both the C&C Servers and effected hosts in a network. Their approach is depends on the observation that, because of the pre-programmed activities related to C&C, bots that has the same Botnet will demonstrate spatial-temporal correlation and similarity. For example, they engage in coordinated communication, propagation, and attack and fraudulent activities. Their prototype system, BotSniffer, can grab the spatial-temporal correlation in network congestion and utilize statistical algorithms to identify Botnets with theoretical bounds on the false positive and false negative rates. They calculated BotSniffer by using many real-world network traces. The consequences show that BotSniffercan detect real-world Botnets with high accuracy and has a very less false positive average.

In the paper [7] reported a vulnerability of the air interface of fourth generation cellular networks, the Long Term Evolution, to Distributed Denial-of-Service (DDoS) attacks launched from Botnets. The attack scenario constitution of a Botmaster instructing the Botnet nodes to start sending through or downloading dummy data for overwhelming the air interface, thereby denial of service for voice users. Through simulation by using a capable LTE simulator, they determine the number of Botnet nodes required per cell that can effectively render the cellular network unusable. Specifically, they show that a Botnet that has spread to only 4% of subscribers is capable of lowering the voice feature from 4.3 to 2.7 in Mean Opinion Score scale of 1 to 5 for the scheduling strategies designed for realtime flow. On the other side, a Botnet that has managed to spread to 7% of subscribers can cause a MOS value of 1, which is a complete outage. The threat identified and the reported consequences can inspire the working of new phenomenon to assure the security and availability of vital telecommunication services.

In the paper [3] proposed a solution of VPN gateway based on the SSL protocol. VPN technology is the use of the knowledge of cryptography in the open and public network to establish a virtual private network. IPSec VPN and SSL VPN are two kinds of VPN technology and products used in most cases currently. IPSec VPN operates at the network layer, SSL VPN works in secure sockets layer. SSL VPN uses a series of cryptographic techniques, including symmetric encryption, asymmetric encryption, digital signatures, digital certificates, as well as message digest algorithm. This article analyzes the principle of VPN technology and the SSL protocol.

4. CONCLUSION

As detection of botnet has been going through using techniques like honeypots, spamming botnet detection, Network-based Botnet detection, Behavior analysis based Botnet detection, but still there is need to emphasize on it. Botnets are one of the most dangerous security threats for the Internet and the personal or desktop computers world, but they are still rare for the mobile world. With the rapidly-growth in popularity of smartphones, such as Android-based phones, attacks on cellular networks and devices have grown in large number and sophistication. In trying to keep pace with them, protectors have been constantly trying to mitigate the wrong intentions of Botnets. We have studied various techniques for botnet and there is a need to introduce a new hybrid scheme by using VPN and provide better prevention from botnet.
REFERENCES


[3] Chen Fei, Wu Kehe, Chen Wei, Zhang Qianyuan, “The research and implementation of the VPN gateway based on SSL” International Conference on Computational and Information Sciences, pp. 1376-1379, 21-23 June 2013.


