Botnet is a computer network that are owned and controlled by an bot attacker. Botnets are one of the most serious threats to today’s internet. Botnet are a major threat to internet because it consists of large pool of compromised computer that are organized by a master. Some model is necessary to develop the intelligence to identify, detect, and mitigate the risk of an attack. E.g Zombie armies carry out sophisticated attacks to disrupt, gather sensitive data or increase armies. Armies are in the 1000’s to cumulative calculating power. Communication network allows bots to evolve on a compromised host. So it became a cybercriminal threat to society. This paper states the motivation change in computer hacking and also systematically to study P2P botnet along multiple dimensions in botnet construction, command and control mechanisms, performance measurements and mitigation approaches.

Key words: P2P, Botnet, Mitigation, Hacking.

1. Introduction

This work deals with security issues in decentralized peer-to-peer (P2P) networks, which are part of extremely distributed systems. All items of knowledge that arises from this analysis are sometimes in special manner, applicable to the opposite types of distributed systems. Discovered data can facilitate North American nation notice some security principles in larger scale, not solely in terms of P2P networks. Today, centralized botnets area unit still wide used. Among them, net relay chat (IRC)-based botnets [55] area unit the foremost widespread ones, that use IRC [33] to facilitate command and management (C&C) communication between bots and botmasters in a very centralized botnet as shown in Fig. 1.1, bots area unit connected to one or many servers to
get commands. This design is straightforward to construct and very economical in distributing botmaster’s commands; but, it's one point of failure - the C&C server. move down the IRC server would cause all the computer to lose contact with their attackers.. Additionally, defenders may also simply monitor the botnet by making a decoy to hitch within the such as IRC channel. In the initial section, basic summary of P2P network types and their properties is given. Individual threats square measure represented intimately. Within the second section, usefulness and practicable of some theoretical DDoS attacks square gauge demonstrated.

The third section is orientating to issues of viruses in P2P networks. Our system for automatic transfer and detection of latest viruses in peer-to-peer networks is given.

The aim of this technique is obtaining precise data regarding state and behavior of P2P networks. noninheritable knowledge oughtfo show USA structureofshared knowledge frommalware purpose of read,whchwilhelp USA produce empiricmodels of worm spreading. Better understanding of latest ways of attackers, their strategies and tools is obtained, supported the results of security analysis of P2P networks. Next step of this method is developing an efficient defense against these ways.

**Botnet Architecture**

![Botnet Architecture Diagram](image-url)
2. Attacking Behaviors

Infect new computers collective engineering and sharing of malicious emails or other electronic communications (i.e. immediate Messaging) Example - electronic message sent with botnet diguised as a harmless attachment. pilfering personal information Keylogger and set-up sniffer technology used on compromised systems to discover on users and compile personal information Phishing and spam proxy Aggregated computing power and proxy capability make allow spammers to contact larger groups without being tracked. Distributed Denial of Service (DDoS) Impair or eliminate availability of a network to extort or disrupt business. Services are go past specific server or cluster of servers in normal consumer – server design. The attacker will take down, modify or counterfeit given service by thriving attack on just one device.

Ebay can serve USA as AN example: throughout thriving DDoS attack on the most server, no visitant is in a position to use services of this web auction centre. All services are closely connected to the server. assaultive the service is equal to assaultive the server [7]. however not in P2P networks. Individual participants is tormented by the attack, however services ar provided y additional of them. So, there is no general result on whole network. Successful attack on one supernode in Gnutella network doesn't affect accessibility of files. Thesole success is obtained by closing down the sole consumer proposing specific file. decentralised P2P networks unfold services among all participants. This should be taken into account throughout security analysis of P2P networks. Our classification of attacks connected to peer-to-peer networks is founding Table one. chosen attacks from table one are going to be mentioned later. Classification of those attacks looks to be a trifle bit inaccurate, owing to their ambiguity. a number of them may belong to additional teams than we have a tendency to mention. Nevertheless, the classification relies on the measurement of impact on the destination cluster (like peer-to-peer users or peer-to-peer network itself) – this means that attack is assessed into the cluster wherever it can do most harm.

2.1 Command And Control (C&C)

Essential for operation and support of botnet .3 designs – Centralized, P2P and irregular Weakest link of the botnet as a result of Elimination of botmaster takes the botnet . High level of activity by botmaster makes them easier to notice than their bots.
2.2 C&C Centralized Model

Simple to deploy, cheap, short latency for giant scale attacks and easiest to eliminate. For centralized botnets, pull mechanism is often used. Take botnets based on HTTP as associate example, usually a botmaster publishes commands on a web page, and bots sporadically visit this web content via HTTP to envision for any command updates. The address of this web content comes with the larva code and can be modified later on by provision associate address ever-changing command. IRC-based botnets is another case of pull C&C mechanism: all bots sporadically hook up with a pre-determined IRC channel, anticipating their botmaster to issue a command in this channel.

C&C Centralized Model Example

3. Peer to Peer Model

Resilient to failures, exhausting to find, exhausting to defend. Hard to launch giant scale attacks as a result of P2P technologies are presently solely capable of supporting terribly tiny teams (< fifty peers). Botnet C&C mechanism is that
the major a part of a botnet style. It directly determines the topology of a botnet; and thence affects the hardiness of a botnet against network/computer failures, security observance and defenses. Traditional botnets, like IRC-based botnets, square measure brought up as centralized botnets since they need a number of central servers wherever all bots hook up with and retrieve commands from. P2P botnets mean that their C&C models square measure P2P-based, i.e. no central server is employed. every larva member acts as each a command distribution server and a consumer WHO receives commands. This explains why P2P botnets square measure typically a lot of resilient against defenses than ancient centralized botnet.

3.1 Pull Mechanism - Command Publishing/Subscribing
In P2P file-sharing systems, a peer sends out a question longing for a file. The query message are passed around within the network in line with AN application dependent routing protocol. If a peer UN agency has the searched file receives the query, it'll respond with a question hit message to the peer UN agency initiates the query. it's straightforward to adopt this idea and use it for botnet C&C communication. Currently, we've not witnessed P2P botnets on unstructured P2P networks yet. But P2P botnets have emerged on DHT-based structured P2P networks, like Trojan. Peacomm botnet [27] and Stormnet [32]. The C&C mechanisms of those 2 botnets area unit similar. They each use the quality Overnet protocol for dominant their larva members. Every larva sporadically queries a search key, that is calculated by a inherent rule. The rule takes the current date and a random range from [0-31] as input to calculate the search key. during this means, once supplying a command, the botmaster must publish it under thirty two completely different keys. This command publishing/subscribing C&C mechanism enforced in Trojan. Peacomm botnet and Stormnet, however, might not offer as sturdy resilience against defenses as botmasters thought. With a duplicate of captured larva code, it's not laborious for defenders to either fathom the question generation algorithmic program, or observe and predict larva queries. This C&C style makes it attainable for defenders to observe or disrupt atiny low set of botnet management communication channels. We’ll offer additional elaborated discussion on this issue.

3.2 Push Mechanism - Command Forwarding
Push mechanism means that once a botmaster problems a command to some bots, and these bots can actively forward the command to others. during this manner, bots can avoid sporadically requesting or checking for brand new command, and hence, reduce the chance of being detected. In a parasite P2P botnet or a leeching P2P botnet, since not all members in
the P2P network belong to the botnet, some peers within the neighboring list might not be larva members. Therefore it's potential that a command isn't forwarded to any bot. To unravel this issue, botmaster might style some methods to extend the chance that the command hits associate actual larva. As an example, when a laptop is compromised and becomes a larva, it will claim that it's some common files available.

Once a larva is attempting to forward a command, it will initiate searches for these common files, and forward the command to those peers showing in the search result. This predefined set of common files behave because the watchwords for the botnet. This approach will increase the command dispersion chance but might offer defenders a clue to spot bots.

For the second issue, exploitation in-band message or out-of-band message to forward a command depends on what the peers within the target list square measure. If a bot just targets its neighboring peers, in-band message would be a decent alternative. A bot may treat a command as a standard question message and send it to all or any its neighboring peers, and suppose these neighboring peers to continue passing on the command within the botnet. The message would appear as a standard question message to benign peers, however it may be taken as a command by larva members. This theme is simple to implement and onerous for defenders to notice, because the command forwarding traffic is mixed with traditional search question traffic.

On the other hand, if the objective list is generated in another ways that, just like the antecedently discussed approaches supported file search results, a larva should contact those peers exploitation out-of-band message: the larva contacts target peers directly, and encodes the command in a very secret channel which might solely be decoded by a bot member. Clearly out-of-band traffic square measure easier to notice, and hence, can disclose the identities of bots UN agency initiate such traffic. Therefore, as we will see, in botnet style, botmasters can invariably face the exchange between potency and detectability of their botnets. The higher than discussion chiefly targeted on unstructured P2P networks, where the question messages area unit flooded to the network. In prearranged P2P networks (e.g., Over net), a question message is forwarded to the nodes whose node IDs area unit closer to the queried hash worth of a file, which implies a question for a similar hash worth is usually forwarded by a similar set of nodes. Therefore, it might be more economical that a larva will generate totally different hash keys related to the same command. During this approach, one command may be forwarded to totally different parts of the network, material possession additional nodes receive the command search question and obtaining the command.
3.3 Communication Protocols
In most cases botnets use well outlined and accepted Communication Protocols. Understanding the communication protocols used helps to (i) verify the origins of a botnet attack and also the package being employed (ii) permit researchers to decipher conversations happening between the bots and also the masters. There square measure 2 main Communication Protocols used for larva attacks: (1) IRC (2) HTTP

3.4 IRC Protocol
IRC Botnets square measure the predominant version IRC primarily designed for one to several conversations however can even handle one to at least one Most company networks due not enable any IRC traffic therefore any IRC requests will verify and external or internal larvaOutbound IRC requests suggests that associate degree already infected laptop on the network Inbound IRC requests mean that a network laptop is being recruited.

3.5 HTTP Protocol
Due to prevalence of HTTP usage it's tougher to trace a botnet that uses HTTP Protocols Using HTTP will permit a botnet to kilt the firewall limitations that obstruct IRC botnets Detecting HTTP botnets is tougher however not not possible since the header fields and therefore the payload don't match usual transmissions .Some new choices rising area unit IM and P2P protocols and expect growth here within the future. HTTP Botnet Example: Fast-flux Networks Commonly used theme Used to management botnets w/ lots of or maybe thousands of nodes.

4. Related Works
P2P botnets, as a brand new sort of botnet, have appeared in recent years and obtained people’s attention. In [27] Grizzard et al., conducted a case study on Trojan. Peacomm botnet. Later on, Holz et al., custom-made following
technique used to mitigate IRC-based botnets and extended it to investigate Storm worm botnets [32]. Trojan. Peacomm botnet and Stormnet area unit 2 typical P2P botnets. Although bots in these 2 botnets area unit infected by 2 completely different malware, Trojan. Peacomm and Storm worm severally, each of their C&C mechanisms are supported Kademlia [38], that may be a DHT routing protocol designed for suburbanized P2P networks. And a botnet protocol that is additionally supported Kademlia was projected by Starnberger et al. [44]. Moreover, to be ready for the future, another botnets whose design is comparable to P2P design, such as a complicated hybrid P2P botnet [50] and super botnet [49], have been presented as well. There are some works on botnet defense and mitigation. Gu et al., proposed 3 botnet detection systems: BotMiner [28] a protocol- and structure-independent botnet detection framework by playacting cross clustercorrelation on captured communication and malicious traffic, BotSniffer [30] a system which will determine botnet C&C channels in a very native space network without any previous information of signatures or C&C server addresses supported the observation that bots among an equivalent botnet can demonstrate spatial-temporal correlation and similarity and BotHunter [29] a larva detection system victimization IDS-Driven Dialog Correlation in step with outlined larva infection dialog model.

5. Conclusion

In this paper, we’ve got provided a study on P2P botnets, a new generation of botnets from multiple dimensions. 1st we tend to mentioned the how P2P botnet will be created. Then we tend to conferred 2 doable C&C mechanisms and the way they will be applied to differing kinds of P2P botnets. A very attention-grabbing finding is that, in contrast to the final understanding that the C&C channels of P2P.botnets square measure more durable to pack up than a centralized botnet, a P2P botnet that depends on publishing/subscribing C&C mechanism will be effectively noncontinuous by index poisoning attacks. additionally, we tend to introduced several metrics to live the effectiveness, potency and strength of P2P botnets. Finally, we tend to realized doable directions for P2P botnet detection.

References


