I J C T A, 10(9), 2017, pp. 557-566 ISSN: 0974-5572
© International Science Press

A Survey on Botnet: Behavior, Life Cycle, Detection and Prevention

Bhan Sengar* and B. Padmavathi**

ABSTRACT

Among the assorted sorts of malware, botnets are rising briskly because of the most serious threat against cyber-security.Botnets supply a distributed platform for many prohibited activities like launchingdistributed denial of service attacks against crucialtargets,malware dissemination, phishing, click fraud etc. Thecharacteristic of botnets is that they use command and control channels through which they will be updated and directed. In recent times, botnet detection has been a noteworthy analysis topicassociated with cyber-threat and cyber-crime interference.The paper clarifies how bots are developed in networks and is a review of botnet behavior, life cycle,detection and prevention. The study summarizes botnet detection techniques in every category and provides a quick comparison.

Keywords: Botnet; Botnet Detection; Botnet Prevention, Cyber-security, Internet Security,

1. INTRODUCTION

Malicious botnet may be a network of compromised computers referred to as “Bots” underneath theremote of a person’s operator referred to as “Botmaster”. The term “Bot” springs from the word “Robot”; and like robots, bots are designed to perform some predefined functions in machine-controlled manner. In different words, the individual bots are programs that run on a bunch pc permitting the botmaster to regulate host actions remotely. Botnets create a major and growing threat against cyber-security as they supply a distributed platform for several cyber-crimes likeDistributed Denial of Service (DDoS) attacks against important targets, malware dissemination, phishing,and click on fraud. Botnet detection has been a significant analysis topic in recent years. Researchers have projected many approaches for botnet detection to combat botnet threat against cyber-security. During this paper, botnet phenomenons are processed and advances in botnet detection techniques arementioned.

This paper classifies botnet detection approaches into four classes: signature-based, anomaly-based, DNS-based, and mining-based. Moreover, it summarizes botnet detection techniques in every category and provides a quick comparison of those techniques.

1.1. Our Contribution

Besides presenting an intensive survey on botnets and their detection mechanisms, we have a tendency to classified botnets supported underlying (C&C) infrastructure similarly. Our survey has detailed description botnet detection and hindrance mechanism. It additionally offers a comparison between current detection techniques as shown in Table one and explains the various makes an attempt to makebotnet behavior models. This paper additionally introduces a ascendible methodology of botnet detection applicable to P2P network.

* M.E C.S, Department of Computer Science, G H Raisoni College of Engineering & Management, Wagholi, Pune, India, *Email: bhanpratap@rediffmail.com*

** Department of Computer Science, G H Raisoni College of Engineering & Management, Wagholi, Pune, India, *Email: b.padmavathi@raisoni.net*

1.2. Objective

The objectiveof this survey is to shed light-weight on botnets threat by providing a transparent back ground and classification on botnets architectures and their behavior, and to explain some security measures that find and mitigate botnets threats.

1.3. Survey Outline

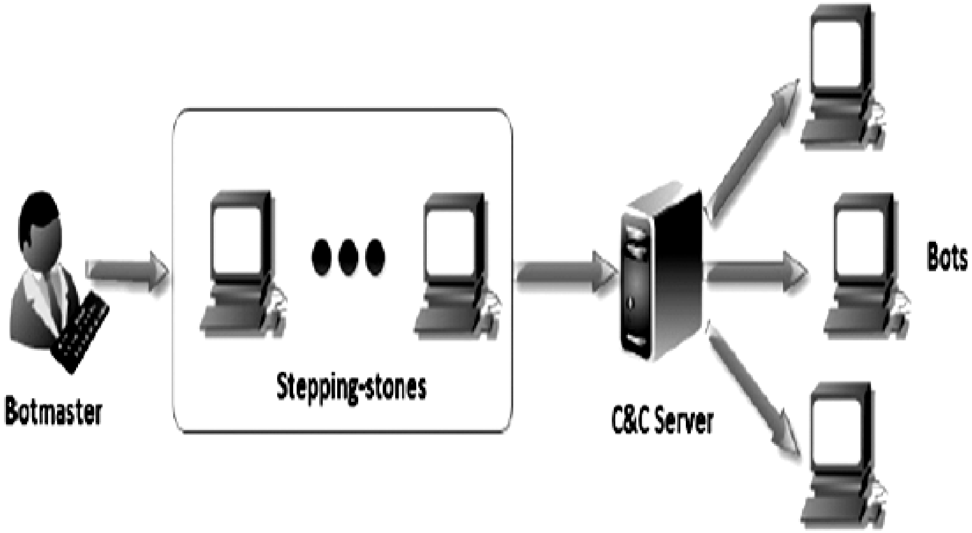
This survey is printed as follows: Section II describes botnet development. During this section, botnet characteristics and botnet life-cycle is explained to supply higher understanding of botnet technology. Section III discussesbotnet varieties. Classifications are based on designof the botnet and underlying network protocol used. In Section IV, four categories of botnet detection approaches together with signature-based, anomaly-based, DNSbased, and mining-based are detailed.Section V provides a short of botnet bar mechanisms. Finally, Section fiveconcludes the survey.

2. BOTNET BEHAVIOUR

2.1. How a botnet works?

In this section, we tend to review the most ideas concerningbotnets that may be utilized in the remainder of the paper. As antecedently expressed, a botnet may be a network of infected machine sunderneath the management of a personality’s operator Two main parts is found among a botnet:thebots and therefore the botmaster. Infected machines are referred to as bots, a term derived from the wordmechanism, reflective the actual fact that each one bots follow the directions given by the human operator, the botmaster, who controls the botnet and utilizes it to achieve the final goal, normally that of ending a security attack against a victim. The botnet is managed through the transmission of Command and control (C&C) messages among its members. To do so, C&C channels should be established. In some cases, bots hook up with a C&C server so as to receive the messages sent by the botmaster. The existence of this server and therefore the design of the C&C communications rely upon the botnet’s own design. Excluding the cited main parts of the botnet, i.e., the botmaster and therefore the bots, alternative roles seem throughout the botnet life-cycle of botnets:

– Developer:This is the person or cluster of individuals UnitedNations agency style and implement the botnet. The developer isn’t essentially a similar person(s) because the botmaster, because the style and implementation work mayare subcontracted. During this line, there exist many malware kits that offer all of the tools needed to create up and administer a particular botnet. They are usually named homemade(DIY) malware creation or generation kits. Many examples is found: Zeus [Fortinet 2010], Twitter [Boyd 2010], Aldi [Danchev 2010], etc.

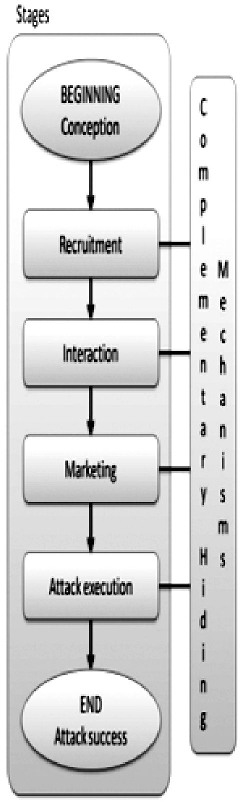


- Client:There exist two main sorts of shoppers of a botnet.Some shoppers rent botnet services from a botmaster samples of such services area unit spam distribution or Distributed Denial of Service (DDoS) execution toa definite server. On the other hand, some clients tries to become botmasters themselves, by gaining control of the botnet by an “illegal” commercial transaction. Subsequently, they use the botnet for their own purposes
- Victim: This is the system, person or network that constitutes the thing of the attack dead. There are many various varieties of victims, looking on the most purpose of the botnet, i.e., a user who receives spam, somebody from whom information is stolen, a corporation that loses manymillion greenbacks owing to a DDoS attack, etc
- Passive participant: This is the owner of a bunch that has been infected and so become a bot. This new bot becomes a part of the botnet while not the user’s consent. This participation, even while not the user’s consent, will result in dramatic legal consequences.

Let us currently target the particular particularities of botnets, accentuation within the initial place a number of the most variations between them and different sorts of malware. These are often summarized as follows: (i) The botmaster will send orders to associate degree infected host while not directly controlling this machine; (ii) bots act during a coordinated manner and follow the botmaster’s directions. This ability to regulate an enormous variety of bots during a coordinated manner allows the botmaster to execute large attacks, like DDoS, click fraud, spam distribution, etc. botnets are designed in such the way that they commit to hide all the above-cited interactions, to hamper botnet detection processes. this can be done using techniques like multi-hopping, ciphering and binary obfuscation. In the next section, these aspects are studied in bigger detail, and our proposal for a brand new taxonomy is explained.

2.2. Botnet life cycle

We propose an in depth study of the botnet life-cycle, starting from its conception to the acheving of the required malicious purpose. The life-cycle planned here may be a linear sequence of stages, i.e., the top of the life-cycle (the successful attack), is reached only after all the previous stages have been successfully carried out.



Botnet conception. This is the primary stage in any botnet life-cycle. The motivation for making a botnet is an important part which will directly have an effect on its style and implementation. various reasons may underlie a developer's call to come up with a botnet. Its main style characteristics area unit outlined during this stage, and these area unit clearly influenced by the particular purpose supposed for the botnet.

Botnet recruitment. Once a botnet is planned and created, there's a requirement for individual bots. Thus, a botmaster should recruit standard hosts as members of the botnet.

Botnet Interaction. This stage involves two completely different processes. First, infected bots should be registered with the botnet so as to include its dynamics and functioning. Second, there should be a communication framework supporting the operation and maintenance of the botnet, in order that the botmaster could confine contact with the various bots. These communications are mostly supported by a C&C channel. The information exchanged constituted of orders (from the botmaster to the bots) and maintenance operations (code change, membership accounting, etc.).

Botnet marketing. Although the foremost common motivationfor a developer to initiate the design and implementation of a botnet is to get financial profit, there ar several alternative attainable reasons together with ego, specific cause, entrance to social teams, etc. regardless of the motivations, there's a selling stage throughout that the botnet should be publicized; the developer has to convey the benefits and capabilities of the botnet in an exceedingly relevant forum so as to cede its use to clients and thus benefit from it.

Attack execution. During this stage, the botmaster orders the bots to perform associate attack. As declared on section above, one among the main feature botnets is that the immense number of bots recruited to hold out the malicious activities. Therefore, botnets are effective weapons for launching attacks that need an oversized range of hosts: DDoS, spam, click fraud, phishing, among others.

Attack success. The final goal of a botnet is to successfully execute the attack it was created for.

3. TYPES OF BOTNET

Botnet classification is straight forward, it uses botnet architecture and the protocols used to control bots as a basis.

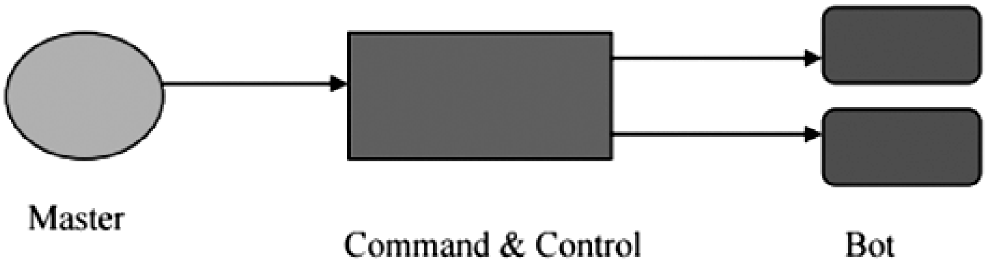
3.1. Classification of botnet according to architecvture

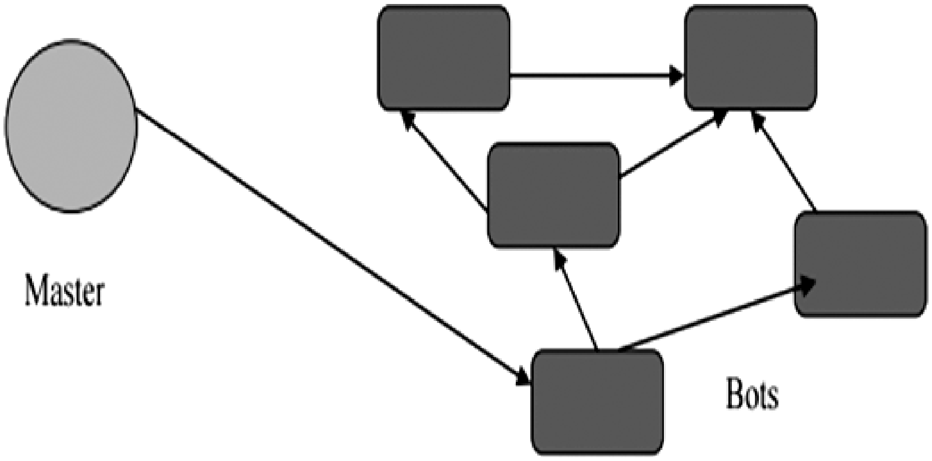
3.1.1. Centralized botnets

In this style of botnet, all computers are connected to one command-and-control center or C&C. The C&C waits for brand new bots to attach, registers them in its information, tracks their standing and sends them commands choosen by owner from a list of bot commands. All zombie computers within the botnet are visible to the C&C. The zombie network owner wants access to the command and center to be able to manage a centralized botnet.

3.1.2. Centralized botnetsDecentralized or P2P (peer-to-peer) botnets

In a decentralized botnet, bots connect with many infected machines on a bot network instead of to a command and centre. Commands are transferred from bot to bot: every bot encompasses a list of many





'neighbours', and any command received by a bot from one in every of its neighbours are going to be sent on to the others, distributing it across the zombie network. During this case, a hacker must have access to a minimum of one pc on the zombie network to be able to control the complete botnet.

3.2. Classification of Botnet According to Network Protocols

- IRC-oriented.: bots were controlled via IRC (Internet Relay Chat) channels.
- IM-oriented. It uses communication channels provided by IM (instant messaging) services such as AOL, MSN, ICQ etc.
- Web-oriented: A bot connects to a predefined net server, receives commands from it and transfers information to that in response.
- Other: Additionally to the botnet types listed above, there are other types of botnets that communicate via their own protocol that solely supports the TCP/IP stack, i.e., they solely use transport-layer protocols like TCP, ICMP and UDP.

4. BOOTNET DETECTION

Despite the long presence of malicious botnets, solely few formal studies have examined the botnet drawback. To date, just little is understood concerning botnet malicious behavior. The Honeynet project was one of the pioneering informal studies of the botnet drawback. However, efforts are ongoing to quantify the botnet problem, notice the presence of botnets, and make a blue print of defenses against attacks by botnets.

Botnet detection and tracking has been a serious analysis topic in recent years. Totally different solutions are proposed in academia. There area chiefly two approaches for botnet detection and tracking. One approach is based on putting in honeynets. This approach is generally helpful to know botnet technology and characteristics.

The other approach for botnet detection relies on passive network traffic monitoring and analysis. Botnet detection techniques based on traffic monitorning are helpful to spot the existence of botnets. These techniques is classified as being signature-based, anomaly-based,DNS-based, and mining-based.

4.1. Signature-based Detection

A signature-based Botnet detection technique uses the signatures of current Botnets for its detection. This technique has many benefits, like terribly lfalse alarm rate, immediate detection, easier to implement and there's higher information regarding the detected attack. Signature based detection is primarily used to detect known botnets.

Thus, unknown botnets cannot be detected by this technique. Anomaly-based detection techniques are introduced to beat this downside.

4.2. Anomaly-based Detection

The main idea behind anomaly-based detection approach is to perform botnet detection by considering many completely different network traffic anomalies, as well as high network latency, high traffic volume, traffic on uncommon ports, and strange system behavior that would indicate the presence of malicious bots within the network.

Anomaly-based detection techniques are divided into host-based detection and network-based detection.

A host-based technique could be a detection strategy that monitors and analyzes the internals of a computer system rather than network traffics on its external interfaces. During this approach the individual machine is monitored to seek out any suspicious behavior, as well as its process overhead, and access to suspicious files. If suspicious activity is detected the Host Intrusion Detection Systems can alert the user or administrator. It takes snapshot of existing system files and matches it to the previous snapshot.If the important system files were changed or deleted, the administrator is alerted.

4.3. DNS-based Detection

DNS-based detection techniques are based on specific DNS info generated by a botnet. DNS-based detection techniques are like anomaly detection techniques as similar anomaly detection algorithms are applied on DNS traffic. Bots usually initiate reference to C&C server to induce commands. so as to access the C&C server bots perform DNS queries to find the various C&C server that's usually hosted by a DDNS supplier. Thus, it's attainable to notice botnet DNS traffic by DNS observation and notice DNS traffic anomalies[15,17].

4.4. Mining-based Detection

One effective technique for botnet detection is to spot botnet C&C traffic. However, botnet C&C traffic is tough to observe. In fact, since botnets utilize traditional protocols for C&C communications, the traffic is comparable to traditional traffic. Moreover, the C&C traffic isn't high volume and doesn't cause high network latency. Therefore, anomaly-based techniques aren't helpful to spot botnet C&C traffic. Many data processing techniques as well as machine learning, classification, and clustering may be used detect botnet C&C traffic.

In 2008, Strayer et al. [32] projected a network-based solution using machine learning techniques for detecting botnet traffic. They showed that proof of botnet command and control activity can be extracted from flow characteristic using passive traffic analysis. They adopt a two stage method that first distinguish IRC flows, so to establish botnet C&C traffic from traditional IRC flows [32]. Though these techniques are effective to detect some botnets, they are specific to IRC-based botnets. Moreover, for correct analysis and detection these techniques need access to payload content. Thus, it cannot detect encrypted C&C traffic.

5. BOTNET PREVENTION METHODS

At present, defense against botnets is usually preventive or defensive. Preventive defense includes proactive measures to avoid botnet infection. Hosts and networks will adopt preventive measures against botnets to boost the bar for attainable botnet infection. These strategies are effective before the botnet infection has taken place.

5.1. Install a Windows Firewall

Though sometimes tempting for end users to disable, a properly configured Windows firewall can block many network-based exploits. This measure is especially appropriate for large agencies with many similarly configured machines.

5.2. Disable AutoRun

The autorun feature, that mechanically installs software system, ought to be disabled to forestall operative systems from blindly launching commands from foreign sources.

5.3. Consider Network Compartmentalization

In most computing environments, workstations don't ought to communicate with one another across departments. closing down this capability goes a protracted method toward preventing the unfold of botnets.IT managers ought to establish personal virtual native space networks (VLANs), or access management lists (ACLs) between sub networks to limit exposure. This strategy isn't an honest match, in environments that mix voice and data communications, as it tends to break the ability to negotiate virtual circuits on the fly.

5.4. Provide Least Privilege

When users aren't administrators of their own workstations, it's more tougher for malware to propagate via drive-by transfer or for AutoRun methods to take on a system. Preventing users from being administrators additionally makes it tougher for his or her user account credentials to unfold malware, should the to the pc become infected.

5.5. Install Host-Based Intrusion Prevention

To keep botnets from taking root in a very system, IT managers ought to concentrate extra protections on specific network layers based on vulnerability, like at points of contact between specific hardware and software.This approach doesn't fix technical flaws or holes in operational systems or application code, however it will cut back the probabilities that exploits are going to be successful. These tools are extremely effective, however they're expensive and difficult to deploy.

5.6. Enhance Monitoring

The more that is known about how end users and the network operate in normal activity, the easier it will be to determine in real-time when a botnet infestation causes slight anomalies. Around-the clock monitoring is ideal, using products that collect data on network traffic, train devices to monitor abnormalities, and detect and prevent intrusions. However, even with remote managed security services filling the gap, enhanced monitoring might be beyond the capabilities of many government agencies.

5.7. Use a Proxy Server

While it's impractical to stop all probably hostile outward-bound traffic, forcing outward-bound traffic through a proxy server offers agencies a secondary choke point for watching and controlling internet access and for defeating some attempt to tunnel around security measures. Content filtering is acceptable for nearly any agency.

5.8. Filter Data Leaving the Network

Botnets generally establish communication with one or a more of remote servers that hackers use to retrieve personal data.To prevent these communications, and also the threats related to them, agencies will command unwanted traffic from going away in the network, a tool referred to as egress filtering. Agencies can force net traffic through proxies or content filters or deploy a data loss interference (DLP) solution.

5.9. Monitor DNS Queries

The way that a digital computer responds to domain name system (DNS) queries is commonly an early indication that the digital computer is also infected. Specifically, responses from workstations that contain terribly low time-to-live (TTL) values ought to be monitored, as low TTL will indicate infection. Monitoring permits system administrator to act before the infection spreads.

6. NEW PROPOSED SYSTEM FOR BOOTNET DETECTION FOR SCALABLE NETWORK

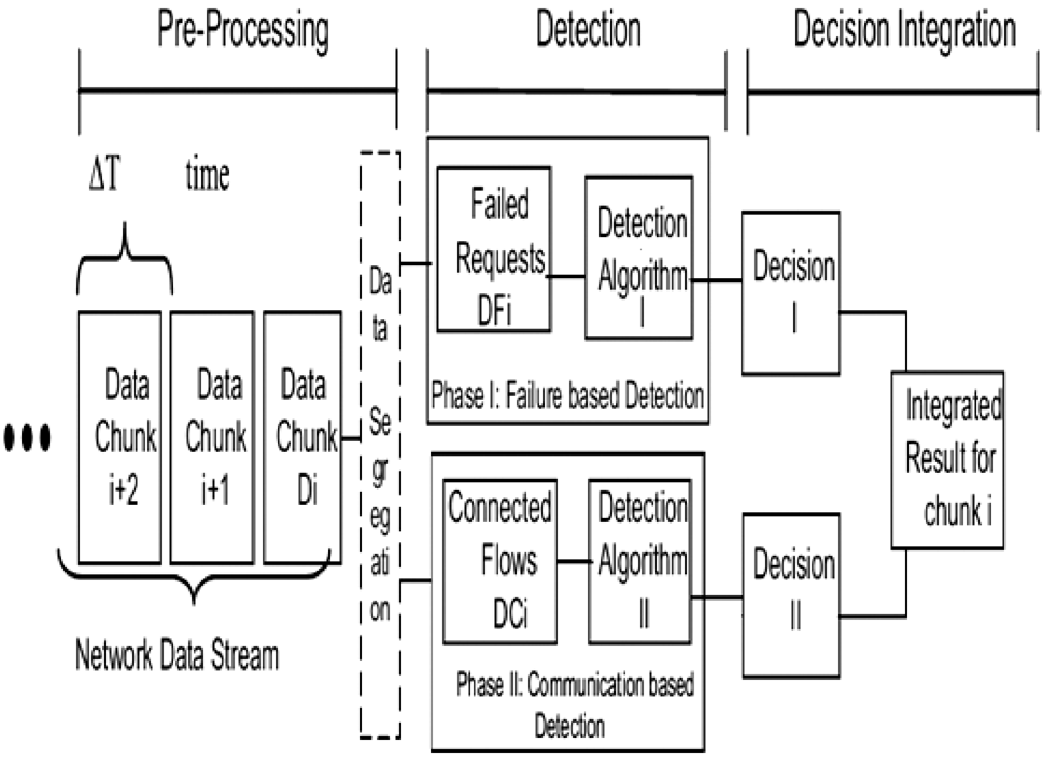
Our research seeks to develop a more systematic and general approach to building a framework for the detection of bots. In this work, the focus is given to designing a bot detection system where network data is captured on the fly for a small time interval.

The bot detection problem is developed as an outlier detection problem within the data stream. The network administrator is instantly notified regarding the infected host. Tt's determined that a bot usually incorporates a completely different network pattern than the traffic generated by regular P2P application traffic. A brand new bot(newly infected system) is useless to its master if it doesn't connect with the botnet. It tries to connect to its botmaster via some rallying mechanism and enlist its neighbors on the network to get the commands. This strategy is named building phase of a botnet where bot generates several fail requests to create the botnet. Once the bot is connected to the botnet, it should not solicit different bots; it keeps communicates with the connected bots that have responded; known as communication phase of a botnet wherever bots and botmaster have a one to one communication.

The suggested system segregates the network traffic into two parts: building phase traffic i.e. failure (request) traffic and communication traffic. Multiple indicators from varied stages of a monitored host facilitate to develop an improved detection system to find if the host is infected. Detection algorithms are deployed in parallel and for higher accuracy, results are integrated into one decision to decide whether a host is bot or not.

This approach makes our proposed solution capable of finding known and unknown bot hosts with proficiently using network traffic characteristics only.The scalability is achieved by developing a cloud-based environment capable of handling huge information from backbone/ISP traffic. The contributions of the planned approach are listed as follows:

- A distinctive bot detection system is made on the essential characteristics of bots, namely, failure traffic and communication traffic. Every section detects the presence of bots separately in parallel, thus reducing the general detection time with high accuracy.
- An on-line larbot detection system is developed that processes the network data in the form of an data stream.
- An effective formula for the detection of bots via network failure traffic solely is planned that is capable of detecting newly infected hosts before they start interacting with the botnet.
- Distributed Hadoop MapReduce paradigm is adopted to process big data and acheive scalability.
- A model framework is employed and evaluated based real-world network traffic, which has demonstrated high accuracy.

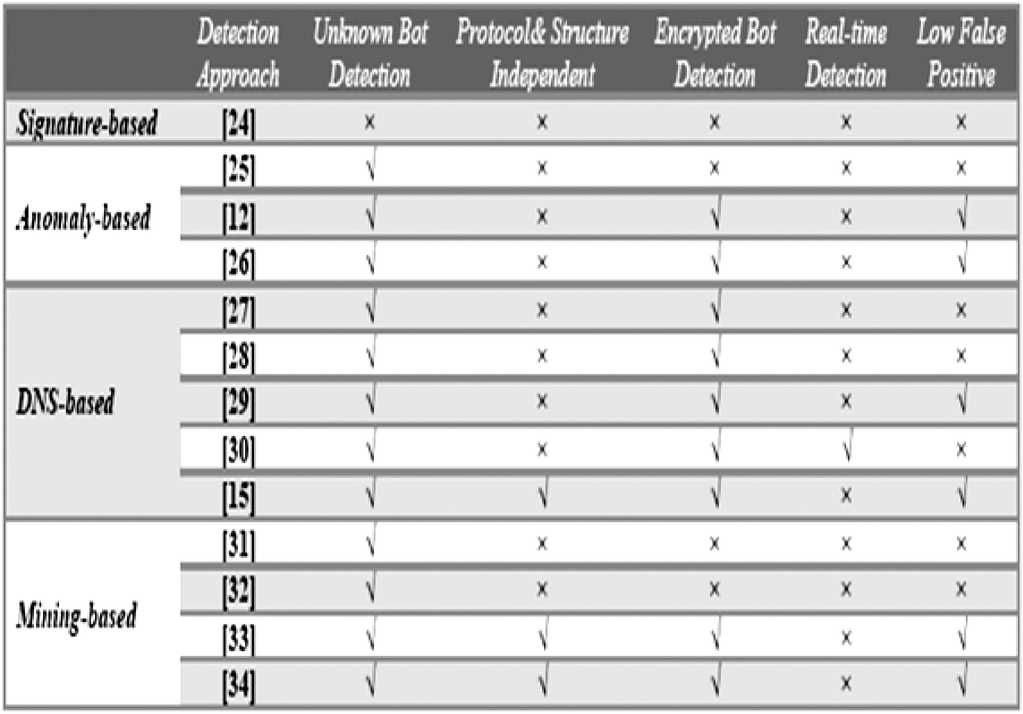


7. CONCLUSION

Despite the fact that our knowledge about botnets is incomplete; botnets are one of the most serious threats to network security. This survey was conducted to better understand botnets and is an attempt to organize the enormous background available in this area to help researchers who are starting in this area.

This section provides a brief comparison of botnet detection techniques. We have compared botnet detection approaches based on key features including: ability to detect unknown bots, capability of botnet

TABLE 1. COMPARISON OF BOTNET DETECTION TECHNIQUES



	Detection Approach	Unknown Bot Detection	Protocol& Structure Independent	Encrypted Bot Detection	Real-time Detection	Low False Positive
Signature-based	[24]	×	×	×	×	×
Anomaly-based	[25]	√	×	×	×	×
	[12]	√	×	√	×	√
	[26]	√	×	√	×	√
DNS-based	[27]	√	×	√	×	×
	[28]	√	×	√	×	×
	[29]	√	×	√	×	√
	[30]	√	×	√	√	×
	[15]	√	√	√	×	√
Mining-based	[31]	√	×	×	×	×
	[32]	√	×	×	×	×
	[33]	√	√	√	×	√
	[34]	√	√	√	×	√

detection regardless of botnet protocol and structure, and botnets with encrypted C&C channels, real-time detection, and accuracy. This comparison is summarized in Table 1.

As Shown in this table, signature-based techniques can only detect known botnets, whereas the other classes are ableto detect unknown bots. However, there are few botnet detection techniques [15, 33, 34] that can detect botnet regardless of botnet protocol and structure. These techniques will be effective even though botmaster's change their C&C communication protocol and structure. On the other hand, detection techniques that require access to C&C payloads [24, 25, 31,32] are less effective as botmaster's tend to use encrypted channels for C&C communications.

Among all detection techniques, the only approach that allows real-time detection is a DNS-based detection which uses DNSBL counter-intelligence to detect reconnaissance in real-time. However, active countermeasures run the risk of false positives. The most recent botnet detection techniques [33, 34] based on data mining as well as DNS-based botnet detection approach in [15] provide promising tradeoff. These methods are independent of botnet protocol and structure. Moreover,they are effective to detect encrypted C&C botnet communication. In overall, these techniques can detect realworld botnets regardless of botnet protocol and structure with a very low false positive rate.

REFERENCES

[1] G. Eason, B. Noble, and I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (*references*)

[2] BOYD, C. 2010. The DIY Twitter Botnet Creator. http://www.gfi.com/blog/the-diy-twitter-botnet-creator/

[3] FORTINET. 2010. Fortinet August Threat Landscape Report Shows Return of Ransomware and Rise of "DoIt-Yourself "Botnets. http://investor.fortinet.com/releasedetail.cfm?releaseid=504094.

[4] DANCHEV, D. 2010. DIY botnet kit spotted in the wild. http://www.zdnet.com/blog/security/diy-botnet-kitspotted-in-the-wild/9440.

[5] H. Choi, H. Lee, H. Lee, and H. Kim, "Botnet Detection by Monitoring Group Activities in DNS Traffic," in Proc. 7th IEEE International Conference on Computer and Information Technology (CIT 2007), 2007, pp.715-720.

[6] P. Vixie, S. Thomson, Y. Rekhter, and J. Bound, "Dynamic updates in the domain name system(dns update)," 1997. http://www.faqs.org/rfcs/rfc2136.html/.

[7] R. Villamarin-Salomon and J.C. Brustoloni, "Identifying Botnets Using Anomaly Detection Techniques Applied to DNS Traffic," in Proc. 5th IEEE Consumer Communications and Networking Conference (CCNC 2008), 2008, pp. 476-481.

[8] W. Strayer, D. Lapsley, B. Walsh, and C. Livadas, Botnet Detection Based on Network Behavior, ser. Advances in Information Security. Springer, 2008, pp. 1-24.