Chapter

Threats from Botnets

Ji Yimu and Liu Shangdong

Abstract

At present, various cyberattacks based on Botnet are the most serious security threats to the Internet. As Botnet continue to evolve and behavioral research on Botnet is inadequate, the question of how to apply some behavioral problems to Botnet research and combine the psychology of the operator to analyze the future trend of Botnet is still a continuous and challenging issue. Botnet is a common computing platform that can be controlled remotely by attackers by invading several noncooperative user terminals in the network space. It is an attacking platform consisting of multiple Bots controlled by a hacker. The classification of Botnet and the working mechanism of Botnet are introduced in this chapter. The threats and the threat evaluation of Botnet are summarized.

Keywords: Botnet, threat evaluation, Botnet classification, Botnet threat

1. Introduction

In 1990, the continuous development of the global economy led to the continuous reform and innovation of information technology, which gave birth to the computer and the Internet, and Internet technology was introduced into every household. In the new century, with the globalization and informatization of network, computer network has become indispensable knowledge for the development of the Internet. At present, the demand of computer network is increasing, and various social organizations such as enterprises, governments, and schools are constantly connecting themselves to the network to exchange and share information resources. With the interconnection of global networks, the Internet is everywhere in the world. From China's core report the 43rd Statistical Report on Internet Development in China [1], we can see the development of the Internet in China and the country's emphasis on the Internet.

The number of Internet users in China has increased gradually from 2007 to 2019, reaching more than 829 million in 2018. The penetration rate of the Internet also increased dramatically year by year. In 2018, the penetration rate was more than 59.6% for the population. It can be seen that the resources of the Internet are accessible to everyone.

The emergence of the Internet has brought a lot of convenience to people's life, but meanwhile, with the continuous expansion of network scale, the security risks have been exposed. For the computer network itself, there are some inherent security risks in design. With the network scale gradually expanding and complex network environment, many criminals make use of the vulnerability on the network for network invasion, information leakage, hacker blackmail, and other attacks. These hazards not only affect people's safe use of the network but also can lead to the disclosure and destruction of sensitive information of enterprises, public

institutions, military, and financial institutions, adversely affecting the national economy and security. According to the data of the 2018 China Internet Cyber Security Report provided by the China National Internet Emergency Center [1], the number of security vulnerabilities collected by the National Information Security Vulnerability Sharing Platform is 14,201 in 2018.

Botnet is a common computing platform which can be controlled remotely by attackers by invading several noncooperative user terminals in network space. "Invading in network space" refers to an area where hackers can enter and exit at will to send arbitrary information and files within an IP block or an Internet region; "noncooperative" means that a vulnerable computer receives no warning notice for the upcoming attack; and "remote control" means that a Botnet usually has a C&C server that can remotely accept control commands from hacker and concurrently send the corresponding instructions in the form of messages to the corresponding infected host (Bot). Over time, a small Bot can be expanded to be a Botnet with thousands of Bots, which, due to the large number of Bots, has high-performance storage size and fast computational response time. Making use of these characteristics, hackers can easily occupy network flow and launch corresponding persistent attacks on a specific target, such as mail attacks, HTTP flooding attacks, etc. At this stage, Botnet has become the main attacking method used by hackers. Due to its simple formation and various types, Botnet has become one of the biggest threats to Internet security and a key research topic by experts.

A Botnet is an attacking platform composed of multiple Bots that is controlled by the commands that hackers send to it, and its behavior is also controlled by hackers. Therefore, the attack of Botnet is generally controlled by the subjective consciousness of the hacker, which leads to the threat generated by it making it hard to locate and predict its threat. From the last century to the present, Botnet attacks not only cause network equipment paralysis but also seriously affect the country at political and economic level, involving military aspects as well. Many newspapers and magazines have published Botnet attacks. In the early twenty-first century, the Conficker Botnet, which was spread by network sharing and U disk, has spread tens of thousands of host computers, and this Botnet mainly made use of the vulnerability MS08–067. During that attack, not only the personal computer was affected, but also the national defense platforms of Germany and the United Kingdom were affected to varying degrees. Some aircrafts were delayed because the attacks prevented releasing of normal commands. In 2016, the United States experienced a large area of network outage, which was caused by a denial-of-service attack on Dyn, a famous American company. The company emphasized that the attack covers millions of IoT devices around the world (the source IPs of UDP/domain name server (DNS) attack are almost fake IPs, so this number does not represent the number of Bots) and some of the important attacks are from IOT devices. Through analysis, the culprit of the incident was the Mirai Botnet, whose source code was published online [2]. According to the 2017 China Internet Security Report, more than 200,000 IP addresses in the Chinese mainland have been affected by hacker attacks, including more than 4000 C&C servers serving to convey commands. These cases show that Botnet poses a serious security threat to China.

China, even the whole world, has paid great attention to the security problems caused by Botnet. In the field of scientific research, on January 23, 2008, the "Seminar of Response to Botnet" sponsored by China National Internet Emergency Center/Coordination Center (CNCERT/CC) was held in Huaxin Building, Beijing. At the International Supply Media Conference held in Nice, France, in 2017, Derek Manky, head of global security strategy of Fortinet, said that the intelligent cluster networks could replace Botnet as a new threat in the future. At the 8th International Conference on Communication and Network Security (ICCNS) in 2018, research

topics such as communication and network security, malware and Botnet, and communication privacy and anonymity were discussed in depth.

There are several reasons why Botnet can become the biggest security threat in the world:

1. The development history of Botnet is divided into two phases. It mainly is a kind of virus or worm in the first phase and transforms into the Botnet platform in the second phase. The advantages of the virus are rapid infection and rapid transmission, but the disadvantages are also obvious, that is, the Bot cannot be controlled by the hacker, the degree of infection cannot be perceived by the hacker, and the infected geographical area is very limited and cannot be expanded on a large scale. In summary, the virus is small scale but uncontrollable. The Botnet combines the advantages of the virus and overcomes the shortcomings of virus, so it is very popular among hackers.

2. The virus attack has the characteristic of integration. Botnet is different, the control command of Botnet is issued by separate C&C server, and the attack and invasion are completed by the controlled Bot. The C&C server and the controlled host will make requests and connections through HTTP packets. In this way, hackers only need to send a few commands to the C&C server to launch diversified forms of attack, which improves the flexibility of Botnet and enhances the concealment of Botnet.

3. Security is the foundation of each computer field, and the development of any field will be accompanied by technical achievements in the security of this field. Because Botnet and security measures are developed in a certain order, Botnet can rise rapidly during this period. In the expansion process of Botnet, the first thing is to find the C&C server, and the hackers will make use of the vulnerability to snatch the control of the host. For example, Mirai Botnet will use the weak password vulnerability to hack into the server's telnet port to gain control of the host; the IRC Botnet will break the shared chat room server for the construction of its own C&C server; due to lack of security awareness of users, some companies' cloud servers are also hacked by hackers and used as C&C server, such as Alibaba Cloud, Tencent Cloud, etc.

4. The Botnet applies the knowledge of the key to the management of the Botnet controller in order to prevent the entire Botnet from being uncontrollable after the C&C server is compromised by security experts, so as to improve its concealment and survivability. For example, in a decentralized Botnet, multiple C&C servers are used for unified control, and encryption technology and authentication technology are used in the process of message transmission between C&C servers; in this way, illegal messages cannot be accepted by the controller so as to prevent replay attacks.

Through the above analysis, the process of defending Botnet can be summarized into five steps: analysis and detection, trusted tracking, measurement, situation prediction, and counterattack. Among them, the "analysis and detection" is to find cues of Botnet from the data flow; the "trusted tracking" is to determine the information source of the Botnet; the "measurement" is to manipulate the architecture, life cycle, and attack process of the Botnet; the "situation prediction" is to evaluate the next activity of the Botnet in advance and to prevent and warn in advance; and the "counterattack" is to reduce its activity and break the C&C server to paralyze the Botnet.

At present, there are many different methods for detecting Botnet. For example, Moheeb and others built a real network flow monitoring system to analyze the flow records, binary file types, Botnet control commands, etc.; Cai [3] evaluated the key behavioral characteristics of HTTP Botnet and designed a detection method for HTTP Botnet based on feature analysis; Song [4] adopted displacement entropy and Kalman filtering to detect and analyze the characteristics of P2P Botnet and proposed the corresponding detection algorithm; XU found that P2P Botnet shows higher robustness when random nodes fail, but the robustness declines rapidly when central nodes fail; and Chen proposed a solution to the problem that HMM method cannot be adopted for flow detection of hierarchical Botnet.

2. Classification of Botnet

Botnet has many types of classification, and it can be divided into centralized Botnet and distributed Botnet according to different operating principles.

1. For centralized Botnet, there is only one C&C server in the whole Botnet platform, and all Bots are connected to the C&C server. C&C server has the right to control all Bots.

2. For distributed Botnet, the Bots will also have message communication between each other. According to different command and control protocols, the centralized Botnet can be classified into three categories: IRC-based Botnet, HTTP Botnet, and custom protocol Botnet [5–7]. According to topological structure, the distributed Botnet can be classified into three categories: structured P2P Botnet, unstructured P2P Botnet, and hierarchical Botnet [8, 9]. **Table 1** lists the classification of some known Botnets. Although there are multiple control servers in some Botnets, such as Mega D and Mariposa [10], Bots do not communicate with each other, and they are still classified into the category of centralized Botnet.

2.1 Centralized Botnet

IRC-based Botnet: In the early days of the Internet, the earliest centralized Botnets were mainly IRC-based Botnets, which mainly used IRC services to communicate between C&C servers and Bots (**Figure 1(a)**). This type of Botnet has a simple structure and adopts the known plaintext protocol [11]. Through the monitoring of activity cycle of the Botnet (such as ports and messages), the characteristics can be clearly identified, and these data flow can be easily filtered out in the

Type	Protocol	Examples
Centralized	IRC-based Botnet	SdBot, AgoBot, GT-Bot, RBot
	HTTP-based Botnet	Rustock, ClickBot, Naz, Zeus, Conficker, Torpig
	Custom protocol Botnet	Mega D, Mariposa
Distributed	Structured P2P Botnet	PhatBot
	Unstructured P2P Botnet	Sinit, Nugache
	Hierarchical Botnet	Waledac, Storm

Table 1.
Classifications of some known Botnets.

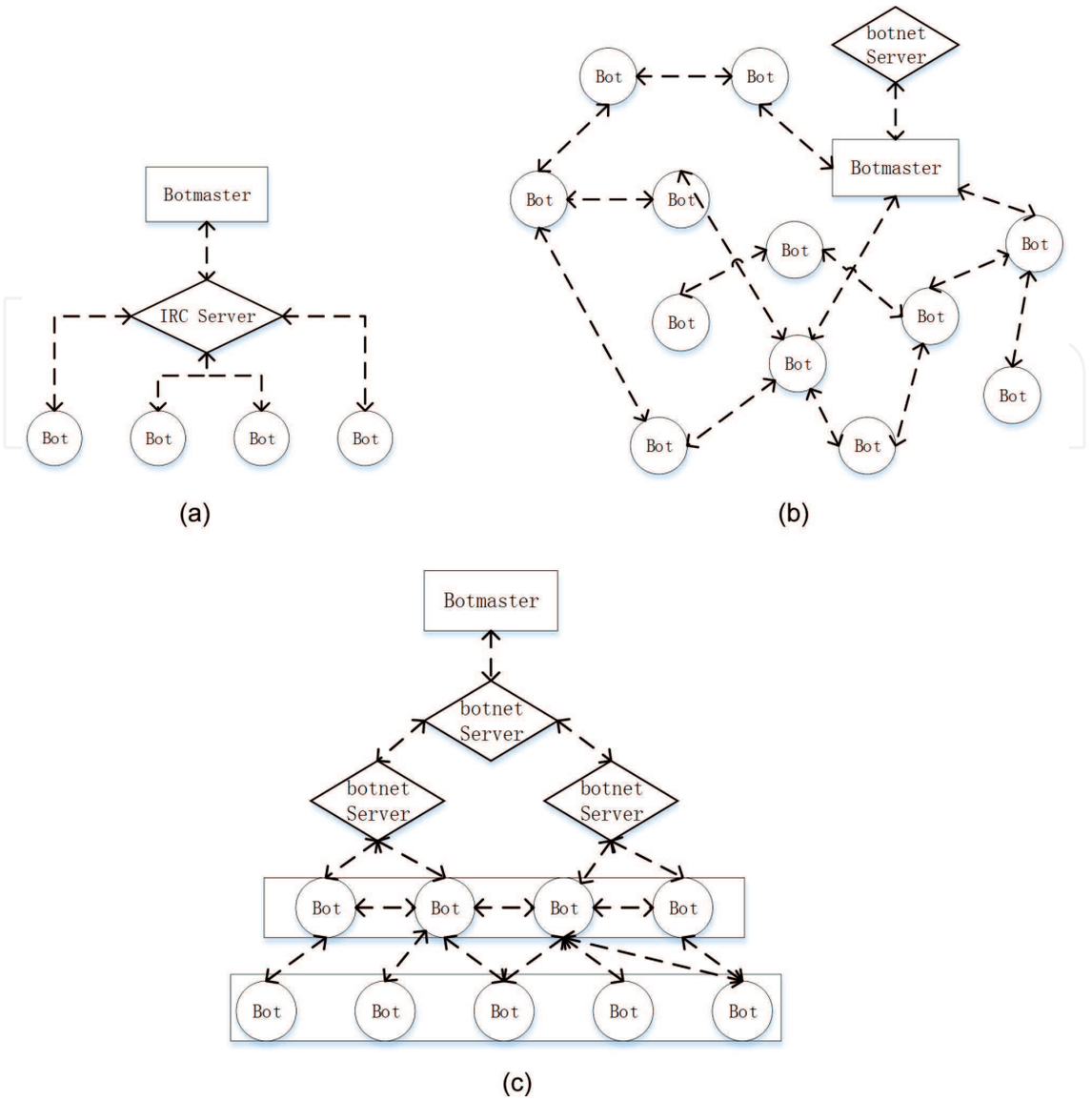

Figure 1.
Three types of Botnet structure.

network defense. This type of Botnet has a little impact because of its small scale. However, due to its simple operating mechanism and strong operability, it is deeply used by hackers. With the current development of Botnet, many hackers still use it.

HTTP-based Botnet: Due to the easy identification of messages of IRC-based Botnet, the HTTP-based Botnet arose. This type of Botnet could hide itself well by adopting HTTP protocol. Since the communication protocols between devices on the Internet are mainly HTTP protocol, HTTP messages in the information transmission of HTTP Botnet can be mixed with normal messages, making it difficult to filter directly through the router rules (ACL), which greatly improves the survival ability of Botnet and makes it more concealable. It is known that the HTTP-based Botnet is more complex and diverse than IRC-based Botnet. Rustock, Zeus, Torpig, etc. encrypt the content of the communication, and Conficker and Torpig also adopt a technique named "domain-flux" to increase the difficulty of blocking their control servers [12]. In addition, a small number of Botnets, such as Naz, also directly use popular social networking sites (such as Facebook, QQ space, etc.) as control servers, increasing the difficulty of detection and blocking [13]. Most Botnets currently use the HTTP protocol.

Custom protocol Botnet: Some Botnets use custom protocols for communication. The known Botnets of this type include Mega D, Mariposa, etc. Since Mega D

uses a custom protocol, the first thing for researchers is to understand its operating mechanism through means of data mining and analysis or reverse capability. Compared with the IRC protocol and the HTTP protocol, Mariposa uses the UDP protocol for transmission, which does not require a three-way handshake. It is more difficult to be shielded by router rules (ACL), and its survivability is stronger.

2.2 Distributed Botnet

For the Botnets described above, the overall structure is a C&C server connected to multiple infected Bots. When the C&C server is broken by security experts, the Botnet is not available anymore. In order to enhance the survivability of Botnets, hackers increase the number of C&C servers and allow Bots to communicate with each other, so the distributed Botnet arise. This type of Botnet has a complicated structure, is difficult to construct, and requires a hacker with strong capabilities. At present, there are many distributed Botnets (such as Waledac and Storm), whose viability has been verified.

Structured P2P Botnet: The communication protocol between such Botnets is not unstructured (P2P protocol). A typical example of structured Botnet is PhatBot, which uses a fully connected Waste Protocol, which leads to a poor scalability of the PhatBot [14]. Early Storm adopted Overnet based on the Kademlia protocol [15] as a way of command and control. Since the information of other nodes can be obtained by the lookup operation in the Kademlia protocol, the researchers could make use of this feature to display the set points in all Overnet networks and then fill in many virtual set points (which we set), so that many messages and file transfers in Botnet will be introduced to the masquerading set points. In this way, the Bots are identified, and the judgment on the scale of Storm Botnet and the defense against it are finally achieved.

Unstructured P2P Botnet: The Bots under this model are connected irregularly, and they can communicate with each other. The communication method is also irregular, and they can send messages in a one-to-many way. There are many types of unstructured P2P Botnets, with two main ones (Nugache and Sinit). The operating mechanism of Sinit is random scanning, which adopts a scan code in the source code to filter some necessary IP segments, aimlessly identify other Bots. The message is sent through port 53, with a poor degree of concealment. The Nugache Botnet keeps a list internally. When the Botnet asks for a connection, it selects an uncertain record from the list of connection. If it is not successful, the random selection will continue; if it is successful, the connecting parties will refresh the list with each other [16]. Dittrich made an effort to keep sending message requests, refresh the list, and enumerate the whole Nugache network by recording and finally draws the structure diagram as shown in **Figure 1(b)**. It is found from the structure diagram that Nugache applies a range interval to the exit and entry massage of the Bot, giving birth to a P2P network with random connectivity. This decentralized topology, combined with the encryption of communications, allows Nugache to have very good concealment and keep a substantial number of active Bots unnoticed for a long time.

Hierarchical Botnet: This type of Botnet is referred to as hybrid P2P Botnet in some literature [17], and it is believed that the most prominent feature is the hierarchical structure. The structure is divided into at least three layers, the Bottom layer is the Bots, the middle layer consists of some Bots or C&C servers with better performance as the medium for information transmission, and the top layer is the core C&C server. This structure can prevent the top layer from being discovered by researchers and achieve more complex functions. Kanich et al.'s further research on Storm found that the Storm is a three-layer Botnet [18]. The Bots in the bottom layer could send HTTP messages, virus information, etc. The Bots can use the Internet to

query other proxies infected host, and the most top hacker server (C&C server) is behind the proxy infected host, with a high degree of concealment.

Waledac is another large-scale hierarchical Botnet, which is also used to send large amounts of spam. Waledac has a similar hierarchical structure as shown in the above (**Figure 1(c)**). It has a structure of one more layer than the ordinary hierarchical structure, and relevant research shows that it is transformed on the basis of the previous hierarchical Botnet. Botmaster is mainly divided into four layers of institutions (from bottom to top for Spammer, Repeater, TSL, UTS). The lower two layers are computer devices with vulnerabilities. The upper two layers are the hierarchical C&C servers used by hackers. The communication method of this Botnet is a technology named fast-flux. The third layer (Repeater) serves as a bridge between the second layer and the fourth layer of Bots, that is, using Bot as a proxy. This is different from the Koobface [19] Botnet, which uses trusted social networking sites, game sites, and other large server devices as its own proxy layer. Waledac is more viable in this way. Nunnery et al.'s research found that Waledac is able to offer two different levels of spam business. Through experiments, the researchers found that due to the diversity of the Bots in the bottom layer of Waledac, it has the function of sending spam, but this ability is not strong, and it is easy to be directly intercepted by some large-scale defense servers; there is also a spam service that can be sent directly by the second layer (TSL) of the Waledac Botnet. This method of sending can dynamically modify the contents of the file to prevent it from being killed by the fixed antivirus software, with high availability. At the same time, in order to further improve the concealment of Botnet and prevent it from being detected by network supervisors, Waledac's internal message transmission mechanism is based on elliptic curve encryption to implement encryption technology. A two-in-one technique (timestamp + public key) is used on the communication between the second and third layers to prevent replay and forgery [20]. In order to prevent security personnel from tracking Botnet, Waledac adopts the detection method of domain name polling to prevent the population of fake nodes [21].

Koobface also adopts an intermediate node as a proxy to hide the control server. But Koobface is notable not for its complex structure but for its numerous functional modules and the way it uses social networking sites to spread its messages. Koobface steals the accounts of social networking sites on Bots, automatically logs in and sends malicious links to friends for transmission, which exploits the trust between social network users. Koobface has a range of modules targeted at almost all major social networks and can force infected users to recognize Captcha images, as well as DNS hijacking, search, hijacking, web server and information theft, etc.

3. Working mechanism of Botnet

As shown in **Figure 2**, the life cycle of a Botnet is divided into six phases: (1) There are many ways for a Botnet to propagate a Bot program, such as page virus, vulnerability attack, email phishing, etc.; (2) If the host is infected, then the Bot program will remain in the system; (3) hosts with vulnerabilities send domain name query to domain name server to obtain IP address of Botnet controller; (4) host with vulnerabilities will connect the Botnet controller and join Botnet; (5) communication connection between Bot and Botnet controller start, as well as the issuance and transmission of commands between attacker and Botnet controller; and (6) the Bot attacks the victim at the command given to the controller.

In phase 1, Botnet adopts email phishing or URL hidden connections to link to some web pages and runs malicious code on the page; this propagation mode is similar to worm propagation mode. Both of them are to attack vulnerable services

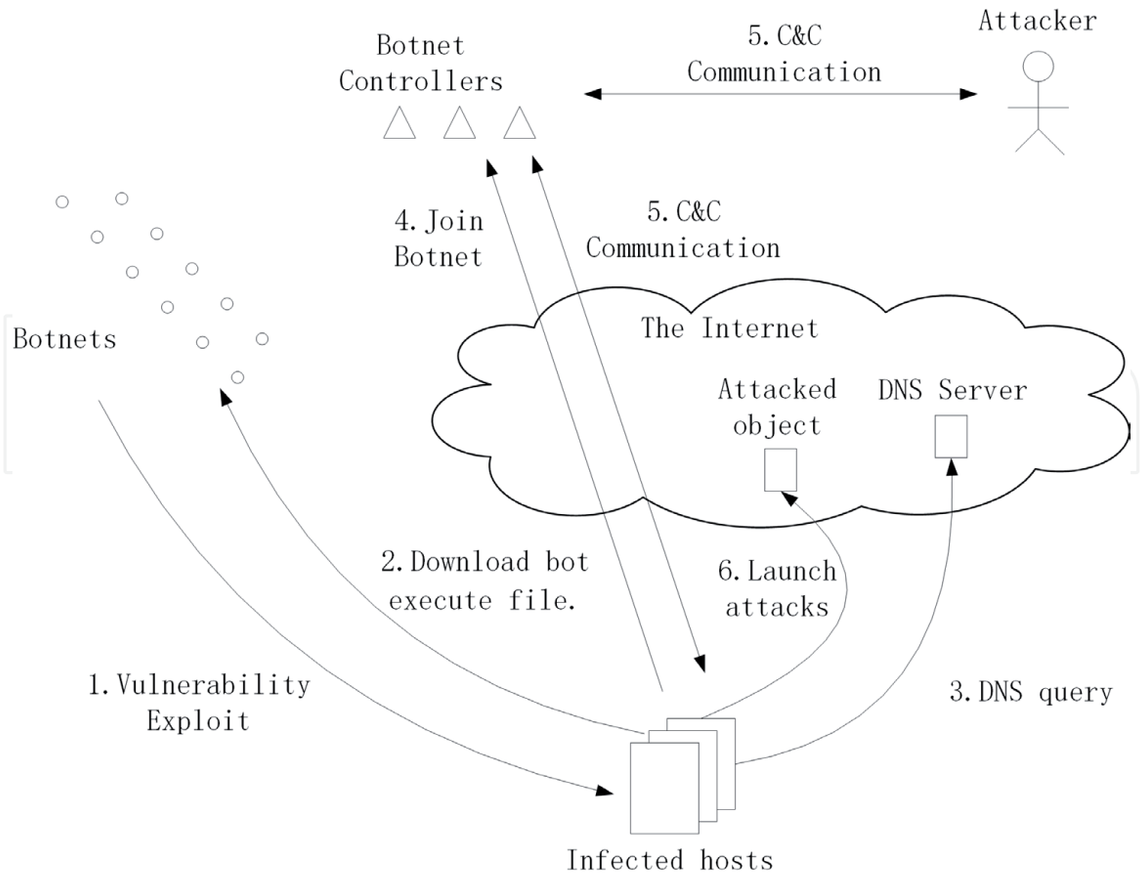

Figure 2.
Working process of Botnet.

by scanning specific ports with specific algorithms, which is very common. There are various algorithms to determine how and when to scan. The Bot does not implement any propagation at first until it receives the command from the attacker, which makes detection more difficult for Botnet [22].

In phase 2, when the computer with vulnerabilities is attacked, it will turn into Bot, and the C&C server will give a command of program installation (such as the echo command in Mirai). This process can be a one-step or multistep installation. For example, a control program is downloaded first, and then the entire Botnet program will be downloaded at a later stage. In addition, some Botnets that exist with chat software will also spread by Relay Node, which is not easy to be found, but also have problems such as delay.

In phase 3, the IP address of the early Botnet controller is directly written in the Bot program, which has the disadvantage of low concealment, so at this stage, the Bot program contacts the C2 controller through the DNS domain name.

In phase 4, because the victim host joined Botnet in different ways, in order to improve the security of the Botnet, it adopts a certain authentication mechanism. Only authenticated hosts can join the Botnet group and carry out communication and control interactions. In addition, the Botnet controller is also selected by the hacker in the Botnet group. In order to prevent these controllers from being shut down or offline, the attacker will generally adopt DNS technology to replace the domain name with a new IP address when the controller goes offline or it is captured. Furthermore, fast-flux technology is used to provide an IP list, and the IP address is periodically bound from the list to the domain name to improve reliability and detection difficulty. The Botnet also replaces the legitimate domain name server on the infected host with its own DNS name server, which has three benefits: (1) if the Bot program is cleared by the host user, some Bots will even reinfect the host through their own DNS name

server; (2) make some antivirus programs unable to update itself; and (3) implement phishing attacks to enable users to access fake websites [23].

In phase 5, the main activity is C&C communication, receiving information sent by the hacker. Botnet maintains communication with the Bot and at the same time protects itself from being captured by the security system. Bot will accept or actively acquire commands, infect more machines, or download updates to the Botnet code. At this stage, due to the original fixed IP, fixed domain name, dynamic update, etc. are less concealed, and Botnet will often adopt domain-flux or fast-flux technology to improve its survivability.

Domain-flux technology is created to solve the problem of central point failure. The attacker uses the domain-flux protocol to prevent itself from shutting down by the defense personnel. The C&C domain name accessed by the Bot is no longer statically hard coded but can be dynamically generated, which allows the C&C server to communicate securely with the Bot [24]. The principle of the domain name algorithm is DGA algorithm, which puts a comprehensive factor such as a dictionary, a random number, a date, and a hot topic into a generation algorithm, generates a string of special character prefixes, and adds a TLD to obtain a final domain name resource. Because of its fast generation speed and high frequency, even with the use of blocking, shielding, and other measures, it cannot protect against invasion. Torpig and Conficker, which appear on the web in general, adopt this technical feature. At the beginning of the twenty-first century, the foundation of fast-flux appeared and gradually attracted more and more attention. Fast-flux is created to address the problem of security personnel locating C&C server domains and IP (both bound to each other) through reverse technology. In general, when a domain name server is used to query the IP of a certain domain name, the result of the query will return the same IP in a short period of time because of the DNS cache. However, fast-flux technology can constantly change the correspondence between IP addresses and domain names, and it makes a large number of queries in a short period of time to return to different results. The fast-flux is divided into two categories (single-flux and double-flux) according to the different number of mapping layers. Single-flux is the fast-flux that has only one mapping layer, a domain name that has one and only one continuously changing IP address. Double-flux represents the fast-flux with two mapping layers. In the actual Internet environment, hackers deploy multiple domain name servers. By modifying the domain name of the top-level server, the correspondence between the IP address of the lower-layer DNS server and the domain name is constantly changing. A Botnet employs fast-flux technology, which would have a large number of C&C servers, and most of the servers are not controlled by the hackers themselves but by Bots. During the check, the security personnel will find that there is no control command from a hacker on the "C&C servers"; these controllers are only responsible for the command forwarding and springboard function, which virtually improves the concealment of the Botnet. Fast-flux technology can also be used to break the domain names of certain phishing websites and malicious websites. Storm adopts this technology to analyze the domain name that sends the message. Phish rock criminal organization adopts it to resolve the domain name of phishing website [25]. Waledac also adopts fast-flux technology to conceal its control server.

In phase 6, the Botnet receives the command sent by the hacker and launches the attack. The attack modes (as shown in **Table 2**) are different [26]; the number of Bots participating in the attack, attack target, and the attack means can also be completely controlled by the hacker. Botnet initially launches a single- or multi-machine distributed denial-of-service attack. Gradually, Botnet turns into profitable attacks, such as stealing users' privacy information on victim machines. For many years, Symantec's global annual cybersecurity report stated that the vast majority of spam is sent by Botnet. Spam sent by Botnet is more harmful than

Attack mode	Difficulty for detection	Complexity	Damage
Small-scale DDoS attack	High	Low	Low
Large-scale DDoS attack	Medium	Medium	High
Stealing information	Low	High	Medium
Sending spam	Medium	Medium	High
Phishing	Medium	High	Medium

Table 2.
Common modes and characteristics of attack initiated by Botnet.

regular spam, making detection more difficult. The process of phishing attack is initiated by Botnet: the Bot erases and replaces the addresses of legitimate DNS on the machine. When the user accesses the confidential page, the replaced domain name server sends the phishing website page to the user [27].

4. Botnet threats and assessment

The threat assessment of traditional Botnet mainly starts from its several key performances; the stronger the key performance of Botnet, the stronger the threat. The key performance indicators of traditional Botnet mainly include four points: transparency, concealment, destruction resistance, and attack capacity.

The transparency of Botnet is mainly reflected in that when an attacker maintains a Botnet or orders a Botnet to attack a certain site, the Botnet can be operated as a whole and there is no need to pay any attention on the internal details of the Botnet. This transparency is mainly realized through the control structure. Attackers input operation commands and control information into the control structure, and the control structure continuously transmits relevant contents to various nodes, so as to control the Botnet as a whole.

The concealment of Botnet means that the activities in the main stages of the life cycle of traditional Botnet need to be carried out covertly, to effectively reduce the possibility of detection of the nodes, operating facilities and overall data flow of Botnet, etc. The concealment of Botnet requires that network nodes should not occupy memory and broadband resources too significantly and the damage to the availability of controlled hosts should be relatively small. The most important thing is to prevent itself from checking by the end user to avoid being discovered by the network security supervision system.

The destruction resistance of Botnet mainly refers to the key characteristic that Botnet is able to maintain its attack ability when some nodes are cleared or destroyed, which is also called tenacity. The great performance of destruction resistance makes the Botnet have strong survivability and can create more superior conditions for the attacker to adjust the behavior characteristics of the Botnet node, thereby effectively avoiding the occurrence of the entire Botnet failure. The main way is to build a more robust structure of Botnet to improve its destruction resistance.

The attack capacity of Botnet mainly refers to the sum of all controllable resources that can be controlled by an attacker. The attack capacity determines the maximum attack strength that an attacker can initiate, and the attack capacity mainly depends on broadband resources and network size. The attack flow that an attacker can initiate increases with the increase of broadband resources. The larger the network size, the more URLs can be exploited by an attacker, and the more dispersed attack source, the fewer constraints in the attack process.

These key performance indicators can be roughly divided into three categories: transparency and concealment belong to the Botnet's defense capability, destruction resistance belongs to the Botnet's survivability, and the attack capacity belongs to the Botnet's attack capability. In addition to the above key performance indicators, there are some more detailed indicators, but they fall within these three capabilities, such as command accessibility of Botnet, node averaging of Botnet, Botnet resilience, etc.

With the rise of the Internet of Things, the rapid development of smart terminals, and the continuous improvement of mobile network technologies, in addition to traditional Botnet, mobile Botnet has become one of the main platforms threatening mobile network security. After the mobile Botnet invades the intelligent terminals in the mobile Internet, these smart terminals are controlled in a one-to-many way through controlling and command channels. It can be seen that mobile Botnet is a subset of traditional Botnet, but it is far more harmful to users than traditional Botnet. Due to the particularity of the mobile network, its threat assessment has its own unique indicators in addition to the key performance indicators of traditional Botnet. The threat assessment for mobile Botnet can be started with the following performance indicators: attack performance, defensive performance, survivability, auxiliary performance, and environmental performance. There are more specific indicators in each performance indicator, such as confidentiality and node control efficiency in attack performance, stability and anti-detection capability in defense capability, network averaging and network connectivity in survivability, propagation capabilities and command mechanism performance in auxiliary performance, scalability and loan consumption in environmental performance, and more.

5. Conclusions

At present, various cyberattacks based on Botnet are the most serious security threats to the Internet. As Botnet continue to evolve and behavioral research on Botnet is inadequate, the question of how to apply some behavioral problems to Botnet research and combine the psychology of the operator to analyze the future trend of Botnet is still a continuous and challenging issue.

Botnet is a common computing platform which can be controlled remotely by attackers by invading several noncooperative user terminals in the network space. It is an attacking platform consisting of multiple Bots controlled by a hacker. The behavior of Botnet is also controlled by the hacker, rather than being controlled by certain code logic, which also makes it difficult to locate and predict the Botnet attack. The Botnet is developed in two phases: it was the primary virus and worm in the first phase, and it transformed into Botnet platform in the second phase. The virus attack has the characteristic of integration. Botnet is different, the control command of Botnet is issued by separate C&C server, and the attack and invasion are completed by the controlled hosts.

Botnet has many types of classification, and it can be divided into centralized Botnet and distributed Botnet according to different operating principles. The difference is that there is only one C&C server in the entire network platform for the centralized Botnet, and the infected nodes also communicate with each other in the distributed Botnet.

The attack process of the Botnet is mainly divided into six phases: in the first phase, Botnet will spread through various traditional viruses or worms; in the second phase, the Bot begins to download the entire Botnet program; in the third phase, the Bot contacts Botnet controller; in the fourth phase, the Bot is authenticated, and the authenticated Bot can join the Botnet group; in the fifth phase, C&C communication

between Botnet and Bot will start to receive information sent by the hacker; and in the sixth phase, the Botnet launches an attack based on commands sent by the hacker.

The Botnet is popular all over the world, which poses a huge threat to the global Internet and the Internet of Things. DDoS attack is still one of the largest Internet security threats in the world, and the DDoS attacks are mainly launched by Botnet.

Acknowledgements

The authors thank Lu Yao, Qing Ye, Na Wang, Yicheng Lu, Haichang Yao, Kui Li, and Ruchuan Wang for their contributions. This work is supported by the National Key Research and Development Program of China (2017YFB1401301, 2017YFB1401302, 2017YFB0202204), the National Natural Science Foundation Program of China (61373017), the Key Research and Development Program of Jiangsu Province (BE2017166), the Natural Science Foundation Outstanding Youth Fund of Jiangsu Province (BK20170100), the Open Fund of Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks (WSNLBZY201514), and the 1311 Project of Nanjing University of Posts and Telecommunications.

Conflict of interest

The authors declare no conflict of interest.

Author details

Ji Yimu[1,2,3,4,5] and Liu Shangdong[1,3,4]*

1 School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, China

2 Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing, Jiangsu, China

3 Institute of High-Performance Computing and Bigdata, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, China

4 Nanjing Center of HPC China, Nanjing, Jiangsu, China

5 Jiangsu HPC and Intelligent Processing Engineer Research Center, Nanjing, Jiangsu, China

*Address all correspondence to: lsd@njupt.edu.cn

References

[1] China Internet Network Information Center. The 43rd Statistical Report on Internet Development in China. 2019;**2**:19-20. DOI: 10.13666/j.cnki.jnlc.2019.02.001

[2] Kolias C, Kambourakis G, Stavrou A, et al. DDoS in the IoT: Mirai and other Botnets. Computer. 2017;**50**(7):80-84. DOI: 10.1109/MC.2017.201

[3] Cai T, Zou F. Detecting HTTP Botnet with clustering network traffic. In: International Conference on Wireless Communications, Networking and Mobile Computing. Shanghai. IEEE. 2012. pp. 1-7. DOI: 10.1109/WiCOM.2012.6478491

[4] Song YZ. P2P Botnet detection based on permutation entropy and multi-sensor data fusion on decision level. Computer Science. 2016;**43**: 141-146. DOI: 10.1145/2379616.2379622

[5] Jianen Y, Zhaoxin Z, Haiyan XU, et al. Detection of IRC Botnet C&C channels using the instruction syntax. Journal of Tsinghua University. 2017;**57**(9):914-920. DOI: 10.16511/j.cnki. cnki.qhdxxb.2017.26.040

[6] Jang DI, Kim M, Jung HC, et al. Analysis of HTTP2P Botnet: Case study waledac. In: IEEE Malaysia International Conference on Communications. 2010. DOI: 10.1109/MICC.2009.5431541

[7] Dibenedetto S, Gadkari K, Diel N, et al. Fingerprinting custom Botnet protocol stacks. In: IEEE Secure Network Protocols. 2010. DOI: 10.1109/NPSEC.2010.5634448

[8] Yu-Peng T, Zhang YZ, Yin T. Modeling and evaluating a cross-realm architecture for P2P Botnet. Acta Electronica Sinica. 2018;**46**(4):791-796. DOI: 10.3969/j.issn.0372-2112.2018.04.004

[9] Wu Z, Zhou H, Yu Z. A novel hierarchical Botnet model. In: IEEE Conference Anthology. China. 2014. DOI: 10.1109/ANTHOLOGY.2013.6784723

[10] Sinha P, Boukhtouta A, Belarde VH, et al. Insights from the analysis of the mariposa Botnet. In: International Conference on Risks & Security of Internet & Systems. Montreal, QC, Canada. 2010. DOI: 10.1109/CRISIS.2010.5764915

[11] Wang T, Yu SZ. Centralized Botnet detection by traffic aggregation. In: IEEE International Symposium on Parallel & Distributed Processing with Applications. Chengdu, Sichuan, China. IEEE; 2009. DOI: 10.1109/ISPA.2009.74

[12] Bonneau J. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. Security & Privacy. San Francisco, CA, USA. IEEE; 2012. DOI: 10.1109/SP.2012.49

[13] Mazurczyk W, Caviglione L. Steganography in modern smartphones and mitigation techniques. IEEE Communication Surveys and Tutorials. 2015;**17**(1):334-357. DOI: 10.1109/COMST.2014.2350994

[14] Barford P, Yegneswaran V. An Inside Look at Botnets. Advances in Information Security. 2007;**33**(4): 171-191. DOI: 10.1007/978-0-387-44599-1_8

[15] Li Z, Chen X. Misusing Kademlia protocol to perform DDoS attacks. In: IEEE International Symposium on Parallel & Distributed Processing with Applications. Sydney, NSW, Australia. 2008. DOI: 10.1109/ISPA.2008.15

[16] Singh K, Guntuku SC, Thakur A, et al. Big data analytics framework for peer-to-peer Botnet detection using random forests. Information Sciences.

2014;**278**:488-497. DOI: 10.1016/j.ins.2014.03.066

[17] Abaid Z, Kaafar MA, Jha S. Early detection of in-the-wild Botnet attacks by exploiting network communication uniformity: An empirical study. In: Ifip Networking Conference. Stockholm, Sweden. 2018. DOI: 10.23919/IFIPNetworking.2017.8264866

[18] Kanich C, Kreibich C, Levchenko K, et al. Spamalytics: An empirical analysis of spam marketing conversion. Communications of the ACM. 2009;**52**(9):99-107. DOI: 10.1145/1562164.1562190

[19] Thomas K, Nicol DM. The Koobface Botnet and the rise of social malware. In: International Conference on Malicious & Unwanted Software. Nancy, Lorraine, France. 2011. DOI: 10.1109/MALWARE.2010.5665793

[20] Rossow C, Andriesse D, Werner T, et al. SoK: P2PWNED - Modeling and evaluating the resilience of peer-to-peer Botnets. In: IEEE Symposium on Security & Privacy. Berkeley, CA, USA. 2013. pp. 97-111. DOI: 10.1109/sp.2013.17

[21] Stringhini G, Hohlfeld O, Kruegel C, et al. The harvester, the botmaster, and the spammer: On the relations between the different actors in the spam landscape. In: Acm Symposium on Information. ACM; 2014. DOI: 10.1145/2590296.2590302

[22] Li Z, Goyal A, Yan C. Honeynet-based Botnet scan traffic analysis. Botnet Detection. 2008. DOI: 10.1007/978-0-387-68768-1_2

[23] Peng T, Harris I, Sawa Y. Detecting phishing attacks using natural language processing and machine learning. In: 2018 IEEE 12th International Conference on Semantic Computing (ICSC). IEEE; Laguna Hills, CA, USA. 2018. DOI: 10.1109/ICSC.2018.00056

[24] Yadav S, Reddy AKK, Reddy ALN, et al. Detecting algorithmically generated domain-flux attacks with DNS traffic analysis. IEEE/ACM Transactions on Networking. 2012;**20**(5):1663-1677. DOI: 10.1109/TNET.2012.2184552

[25] Cook DL, Gurbani VK, Daniluk M. Phishwish: A simple and stateless phishing filter. Security & Communication Networks. 2010;**2**(1):29-43. DOI: 10.1002/sec.45

[26] Khattak S, Ramay NR, Khan KR, et al. A taxonomy of Botnet behavior, detection, and Defense. IEEE Communication Surveys and Tutorials. 2014;**16**(2):898-924. DOI: 10.1109/SURV.2013.091213.00134

[27] Tanner BK, Warner G, Stern H. Koobface: The Evolution of the Social Botnet. Ecrime Researchers Summit. 2010. pp. 1-10. DOI: 10.1109/ecrime.2010.5706694