ANALYSIS OF BOTNETS THROUGH LIFE-CYCLE

R. A. Rodríguez-Gómez, G. Maciá-Fernández and P. García-Teodoro
CITIC-Department of Signal Theory, Telematics and Communications, University of Granada
C/Periodista Daniel Saucedo Aranda s/n E-18071, Granada, Spain

Keywords: Botnets, Security attacks, Network security.

Abstract: Among all the existent threats to cybersecurity, botnets are clearly situated in the top list. As a consequence of this importance, the research community is enormously increasing its interest on this problem and the number of publications on botnets is exponentially growing in the last years. We perform an analysis of botnets aimed at giving order to all these research contributions.

This analysis is different from the previous contributions because it considers the problem of botnets from a global perspective, and not only studying certain technical aspects like type of architecture, protocols or detection techniques. The starting point to do this is the own botnet life-cycle, understood as the sequence of stages that a botnet should successfully traverse in order to reach the success. As a consequence of our study, we have deducted that the interruption of any of the stages makes it possible to thwart a botnet purpose and, thus, make it useless.

1 INTRODUCTION

Botnets are nowadays one of the most serious threats to cybersecurity. The term botnet is used to define a network of infected machines, called bots, which are under the control of a human operator commonly known as botmaster. Bots are used to carry out a wide variety of malicious and harmful actions against systems and services: DoS attacks, spam distribution, phishing and click fraud, among others (Feily et al., 2009). As an example of the relevance of botnets deployment, the FBI (Federal Bureau of Investigation) has recently uncovered more than $20 million in economic losses in the USA. In one case, a victim confirmed damages of nearly $20,000 due to denial of service attacks committed from botnets (FBI, 2007).

Economical profits are also usually behind the design and development of botnets by botmasters. They can reportedly make large sums of money by marketing their technical services. One example of that is Jeanson Ancheta, a 21-year-old hacker member of a group called the “Botmaster Underground”. He received more than $100,000 from different Internet advertising companies using his botnet with more than 400,000 vulnerable PCs (Wilson, 2007).

To understand the scope and thus the threat botnets represent, let us point out that Vinton Cerf, one of the “fathers of the Internet”, estimated that between 100 million and 150 million of the 600 million hosts on the Internet were part of a botnet (Weber, 2007). This represents a 16–25% of the total of computers connected to the Internet.

As a consequence of the impact of botnets, the research community is increasing its interest in this field. The number of publications on botnets has exponentially grown in the last decade, from only a few in earliest 2000 to several hundreds in the last year.

Taxonomies on botnets have been proposed, e.g. (Dagon et al., 2007). They all seem to put their focus on the different aspects of botnets, like architecture, communication protocols, detection techniques, etc., presenting a separate taxonomy for every one of these aspects. Due to this fact, despite these taxonomies allow to understand certain aspects of botnets, it is difficult to get a complete vision of the problem from them.

For this reason, there is a need to contribute a deep analysis that deal with the botnet problem from a global perspective. This study should help to give order to the huge amount of recent research efforts in this field, while the principal concerns and challenges in botnets are highlighted.

In this context, we suggest that it is useful to model a botnet from a product life-cycle perspective. As we extensively describe in this paper, the botnet life-cycle begins with the conception of the botnet, and has the final objective of carrying out a certain attack. We claim that this life-cycle is linear composed

Rodríguez-Gómez R., Maciá-Fernández G. and García-Teodoro P..
ANALYSIS OF BOTNETS THROUGH LIFE-CYCLE.
DOI: 10.5220/0003454402570262
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2011), pages 257-262
ISBN: 978-989-8425-71-3

of a set of different stages that are traversed during the evolution of the botnet.

Observing a botnet from a product life-cycle perspective allows us not only to understand the process of creation, development, integration and use of a botnet, but also to organize the huge number of efforts from the research community in defeating botnets.

More important, as it will be explained in the rest of the paper, this work has leaded us to understand that any defense technique or measure should be designed with this idea in mind: ”interrupting the execution of any of the stages in the botnet life-cycle makes the whole botnet useless”.

Taking into consideration the aforementioned issues, in Section 2 we show our proposal of botnet life-cycle, describing the different stages that compose it and the main conclusions and contributions of this work are summarized in Section 3.

2 BOTNET LIFE-CYCLE

Although we explore here the utilization of a botnet life-cycle as a leverage for the analysis of this problem, this concept has been already proposed in the literature. In effect, some papers has already cited the concept of a botnet life-cycle (Feily et al., 2009) (Liu et al., 2009). However, these studies merely illustrate some of the processes involved in the normal operation of a botnet and, as a result, there is no uniformity either in the stages composing the life-cycle or in the interaction between these stages. In other words, to our knowledge, there is no deep study at this moment about which these stages are, how they should be characterized, and how they delimit between them.

The life-cycle proposed here is a linear sequence of stages. Thus, the end of the life-cycle, *i.e.*, the attack success, is reached only after all the previous stages have been successfully carried out. Specifically, this life-cycle is compose of six stages: *conception*, *recruitment*, *interaction*, *marketing*, *attack execution* and *attack success*. There also exist a series of complementary mechanisms to the stages of the botnet life-cycle. These mechanisms are usually focused on trying to hide the botnet from security officer’s eyes.

It must be noticed that each stage in the life-cycle only represents the beginning of the execution for a specific process. It is obvious that although a botnet reaches the *attack success* stage, at the same time new bots will continuously be recruited (recruitment stage) and controlled (interaction stage). For this reason, it should be clear in our model that any process contained in that stage might be re-executed afterwards.

Once that the botnet life-cycle is established, it is important to point out that any effort in defeating a botnet is really focused on a specific process in some of the referred stages. Thus, it could be deduced that an imaginary efficient measure that prevents any of the cited stages from being executed is enough to avoid the botnet success, *e.g.*, if a measure avoids the infection of bots it would be impossible to recruit enough soldiers to carry out the attack. In summary, we claim that ***interrupting the execution of only one stage in the botnet life-cycle makes the whole botnet useless.***

In what follows, the different stages and processes of the proposed life-cycle are described in detail, referring to the different alternatives in design and implementation that botnet’s developers may follow.

2.1 Conception Stage

The first stage of the proposed life-cycle is the *conception* of the botnet. It is important to understand the reasons that lay behind botnets creation, as well as their usual architectures and designs.

The botnet conception stage can be divided into three phases or processes: *motivation*, *design* and *implementation*. First, a potential botmaster (person who manages the bots) needs a good reason to create a botnet. The motivations of a botmaster could be classified as (Project, 2004): Money, Entertainment, Ego, Cause, Entrance to social groups, and Status, which form the allegoric acronym MEECES. However, the major motivations are those related to economical profit.

Whatever the reasons of potential botmasters are, the process which follows the motivation is to design and implement the desired botnet. Several aspects should be carefully considered during this process, especially those regarding bots infection and botnet communications. They all will be described in the next sub-sections. However, a key decision on the design should be introduced at this point: the architecture of the botnet. This architecture could be: *centralized*, bots are managed through an unique command and control (C&C) server, *distributed*, all the bots of the botnet act simultaneously as servers and clients, or *hybrid*, one or more distributed networks, each one with one or more C&C servers.

Once the botnet is conceptually conceived and designed, the last process of this stage is the own implementation of the bot code, following a traditional software development process.

2.1.1 Defenses focused on the Conception Stage

It seems clear that avoiding to give a good motivation to a potential botnet developer would be a good defense scheme. The same happens if we would be able to impede anybody to design or implement a botnet. In this line, saying that it seems uneasy to have a direct contact with potential botmasters, we consider that the design of legal measures trying to frustrate people about working on botnets is a realistic measure to fight botnets at the conception stage.

2.2 Recruitment Stage

The implemented botnet software will be deployed for its operation in a real environment. For that purpose, some bots should be recruited. Indeed, the aim of the botmaster is to to find the maximum number of vulnerable systems, in order to install his bot. Note that this problem is not particular of botnets, but common to many cyberattacks. In fact, the recruitment, also known as *infection*, has been widely studied in the specialized literature.

There are no special techniques used in botnets, in difference with spreading of viruses or worms. In fact, bot software is considered by many authors as a worm, due to its capabilities of self-replication and propagation.

In order to increase the propagation capabilities of a bot software, it is usually designed to incorporate many existent exploits and even new and not reported bugs (zero-day exploits). To be aware of this problem, let us say that more than 16,000 vulnerabilities have been published in the last three years (NVD, 2010). As an example, Stuxnet botnet (Chien, 2010) was recently designed for exploiting bugs in SCADA systems existing in nuclear plants. It is also remarkable that Agobot botnet (Barford and Yegneswaran, 2007) uses more than 10 exploits.

Botnet malware infection origins are heterogeneous. A user may be infected from the execution of an attached file in a fake email, or opening a resource downloaded from a P2P network. Recently, the propagation of malware through social networks is growing enormously (Faghani and Saidi, 2009).

2.2.1 Defenses focused on the Recruitment Stage

There are many efforts from research community trying to avoid the infection of hosts in the Internet. When applied to the botnet problem, all these techniques are focused on the recruitment stage. If any of them would be completely effective, there would be no way for botmasters to build a botnet.

2.3 Interaction Stage

This stage refers to all the interactions performed during the botnet operation. One of the main differences between botnets and other type of malwares is the existence of communications by using C&C messages. These are of special relevance and a great amount of research papers on botnets are directly related with this aspect. This makes the botnet interaction stage a principal concern for the research community.

The processes involved in this third stage can be classified as *internal* and *external*.

2.3.1 Internal Interactions

Internal interactions are those carried out between members of the botnet, *i.e.*, from the botmaster to the bots or vice versa, or only between bots. Here, we find two processes: *registration* and *C&C communications*.

Registration Process. Registration is the process through which a compromised host becomes an effective part of the botnet. Among all the techniques observed in the different studied botnets, there exists two types of registrations: *static* and *dynamic*.

In the static registration, all the necessary information to become part of the botnet is hardcoded. Usually, the IP address of the C&C server is provided (with some type of obfuscation) in the code of the bots. GT-Bot, Agobot and SDbot (Liu et al., 2009) are some examples of this, among others.

In the dynamic registration, bots have to explicitly request the necessary information to become part of the botnet to a neutral third party or network. An example of this kind of registration is that used in Phatbot (Stewart, 2004c), which utilizes Gnutella cache servers to download a list of peers that belong to the network.

C&C Communications. The bulk of the interactions in the botnet occur after the registration process is completed. These interactions are the C&C communications, which we group attending to two characteristics:

- *Direction of the Information*. According to the direction of the information, C&C messages can be classified as *pull* or *push* (Gu et al., 2008). The bots periodically request information in pull C&C messages, while they receive the information in a passive manner, without explicitly sending a previous request in the push C&C case.
- *Communication Protocol*. Another relevant characteristic regarding C&C messages is the protocol

or protocols involved in the communications. The most commonly observed possibilities in this line are IRC, HTTP, and P2P.

2.3.2 External Interactions

External interactions are those related to communications carried out between a member of the botnet and a non-compromised host. These usually correspond to the access to common services offered in the Internet.

The main external service used by botnets is DNS. In a centralized botnet, bots usually launch DNS queries to resolve the IP address of the C&C server. This is the case of the majority of IRC botnets, like Agobot, GT-Bot or SDBot (Barford and Yegneswaran, 2007) among others. We can also find several examples of HTTP botnets, like Bobax (Stewart, 2004a).

Another common external interaction is the use of P2P networks as an intermediate layer to hide C&C communications. For example, Trojan.Peacomm (Grizzard et al., 2007) carries out searches in the Overnet network looking for files containing URLs from which bots will download an update file.

2.3.3 Defenses focused on the Interaction Stage

As we claim, if we would be able to develop a defense scheme able to interfere in the processes involved in the interaction stage, the botnet would be defeated.

The principal contributions in the interaction stage are about botnet detection. This is due to the fact that if we detect the compromised machines we will be able to avoid its participation in the botnet. As a example of the detection of centralized botnets we can cite (Goebel and Holz, 2007) (for IRC based botnets) and (Chen et al., 2010) (for HTTP based botnets). On the other hand, we also find several papers detecting distributed or hybrid botnet (Kang and Song, 2010).

2.4 Marketing Stage

At this point, the botnet has been created and it is plenty of functionality after the previous stages. Now, the botmaster needs some motivation to use it. Although there are a lot of possible reasons for that (entertainment, ego, status, etc.), the most common is that of earning money.

The expected economical profit is usually obtained by *(i)* selling the botnet code or, most commonly, by *(ii)* renting the botnet code or its services. In both cases, an advertisement procedure is needed, through which the malicious user announces the capabilities and the services offered by the botnet.

The sale of the bot code is one option by botnet developers. Any user with a minimum specialized knowledge can create a botnet if the bot code is available. The kit of Zeus botnet is announced in the underground community forums for about $700.

Other botnet marketing option is the renting of services provided by the botnet. In this alternative, a set of different services could be contracted. A report from Namestnikov, Karspersky Lab (Namestnikov, 2009), presents a list of prices for renting services of a botnet:

- *DDoS Attacks*. This kind of attack costs from $50 to thousands of dollars per day, mainly depending on the size of the botnet and, thus, the strength of the attack.
- *Sending of Spam email*. Sending spam email to a list of around a million of addresses ranges from $150 to $200.
- *Fast-flux Networks*. Cybercriminals, mostly phishers, pay botnet owners $1000 to $2000 per month for hosting fast-flux services.

2.4.1 Defenses focused on the Marketing Stage

Working on defense schemes based on the marketing stage is crucial to undermine the effects of botnets. Obviously, legal penalties to those who advertise botnets help to fight them. Furthermore, measures in the marketing stage should also focus on capturing botmasters activity. We can find the case of Thomas James Frederick Smith in (FBI, 2010), who was one of the creators of *NETTICK*, an IRC botnet. He posted a public message on several forums in which he offered an executable program to control his botnet for $750. He pleaded guilty in June 10th 2010.

Therefore, we firmly think that this stage represents a key point for improving the prevention of appearance of new botnets.

2.5 Attack Execution Stage

The final goal of a botnet is the execution of an attack. The main feature of botnet attacks is the enormous amount of attackers that take part on them. Thus, the principal attacks launched by botnets are:

- *Distributed Denial-of-service (DDoS)*. Denial-of-service (DoS) attacks are attempts to prevent the legitimate use of a service or simply reduce its availability. Distributed DoS attacks (DDoS) are a particular case, in which multiple attacking entities operate simultaneously to attain this goal (Mirkovic and Reiher, 2004). Botnets fit perfectly for striking DDoS attacks. Examples of botnets used for DDoS are Spybot and Agobot (Barford and Yegneswaran, 2007).

- *Spamming*. A spam email contains certain information crafted to be delivered to a large number of recipients, in spite of their wishes (Cormack, 2008). The use of a botnet considerably increases the power to send lots of spam emails in few seconds. Bobax is a botnet used for this purpose (Stewart, 2004b).
- *Phishing*. This is a fraudulent activity defined as the act of conning a person into divulging sensitive information (Levy, 2004). This could be done by means of a replica of an existing web page. To hide these replicas phishers are recently using botnets as fast-flux networks (explained in Section 2.6). As an example, the Storm botnet (Porras et al., 2007) implements this mechanism to hide its binary updating.
- *Click Fraud*. It consists of deceptively clicking on online ads or visiting certain websites with the intention of either increasing third-party website revenues or exhausting an advertiser's budget (Wilbur and Zhu, 2009). The use of botnets allows to simulate the behavior of millions of legitimate users, thus being ideal for this kind of attack (Daswani and Stoppelman, 2007).

2.5.1 Defenses focused on the Attack Stage

A lot of efforts have been done by the research community to deal with the aforementioned kinds of attacks. Many contributions have been given in the prevention, detection and response to these attacks although, regretfully, this is still an open field.

2.6 Complementary Hiding Mechanisms

Complementary hiding mechanism are also considered as part of the proposed botnet life-cycle, although they are not defined as an stage. These are mechanisms designed for hiding the botnet and making it difficult to discover its components (bots, botmaster, C&C channels). Regretfully, even if we were able to disclose a hiding mechanism we have not still defeated the botnet. For this reason, we consider these mechanisms not as an stage, but complementary to them.

There are many possible hiding techniques studied in the literature. We now present those which are widely used in botnets:

- *Ciphering*. Regarding the interaction stage, C&C communication are usually ciphered in modern botnets to prevent them from being analyzed. The development of liable techniques for detection of C&C communications becomes increasingly difficult when ciphering is used. SpamThru (Stewart, 2006) and Zeus (Stewart, 2010) use encrypted channels.
- *Polymorphism*. It consists of creating different versions of the source code of a program to change while its functionality remains. This technique makes the signature-based detection process used by most of current antivirus tools more difficult. Phatbot (Stewart, 2004c) and Zeus (Stewart, 2010) botnets use this technique.
- *IP Spoofing*. It consists of sending IP packets with a fake source address. It is widely used in DoS attacks with the aim of avoiding IP filters.
- *E-mail Spoofing*. Similarly to IP spoofing, e-mail spoofing consists of sending an e-mail with fake sender address (or other fields of the header). This is commonly used in phishing attacks, like that perpetrated by the Bobax botnet (Stewart, 2004b).
- *Fast-flux Network*. This technique allows hiding any final host in the network by means of a big number of proxies that redirect the requests coming from users. These proxies change very frequently by the use of DNS entries with low TTL, thus making to trace the communications difficult. This technique could be use to hide a central C&C server in a botnet.

3 CONCLUSIONS

As a consequence of the impact of botnets, the research community is increasing its interest in this field. In this context, we carry out an analysis of botnets with a double aim: *(i)* to consider the botnet problem in a global scope, and *(ii)* to be an useful tool to make the comprehension of the wide variety of existent botnets easier.

This study is based on a sequential life-cycle, in which every stage is a fundamental part of the botnet life. In consequence, the interruption of only one stage in the botnet life-cycle makes the whole botnet useless. So, we claim that all the defense efforts of the research community are focused on one or more of these stages.

Finally, in our study we highlight the marketing stage. This could represent a key point for improving the prevention of appearance of new botnets. In this line, we emphasize that there is a need for studies in this field in the sense of how a botmaster sells the services of a botnet, the forums in which this information is published, the way that clients access to these forums, etc.

ACKNOWLEDGEMENTS

This work has been partially supported by Spanish MCIN under project TEC2008-06663-C03-02.

REFERENCES

Barford, P. and Yegneswaran, V. (2007). An inside look at botnets. In *Malware Detection*, volume 27 of *Advances in Information Security*, chapter 8, pages 171–191. Springer US, Boston, MA.

Chen, C.-M., Ou, Y.-H., and Tsai, Y.-C. (2010). Web botnet detection based on flow information. In *Computer Symposium (ICS), 2010 International*, pages 381–384.

Chien, E. (2010). W32.stuxnet dossier. Technical report, Symantec.

Cormack, G. V. (2008). Email spam filtering: A systematic review. *Found. Trends Inf. Retr.*, 1:335–455.

Dagon, D., Gu, G., Lee, C., and Lee, W. (2007). A taxonomy of botnet structures. In *Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual*, pages 325–339.

Daswani, N. and Stoppelman, M. (2007). The anatomy of clickbot.a. In *Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets*, Berkeley, CA, USA. USENIX Association.

Faghani, M. and Saidi, H. (2009). Malware propagation in online social networks. In *Malicious and Unwanted Software (MALWARE), 2009 4th International Conference on*, pages 8–14.

FBI (2007). Over one million potential victims of botnet cyber crime. Technical report, FBI Press Release.

FBI (2010). Another pleads guilty in botnet hacking conspiracy. Technical report, FBI Press Release.

Feily, M., Shahrestani, A., and Ramadass, S. (2009). A Survey of Botnet and Botnet Detection. *SECURWARE*.

Goebel, J. and Holz, T. (2007). Rishi: identify bot contaminated hosts by irc nickname evaluation. In *Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets*, Berkeley, CA, USA. USENIX Association.

Grizzard, J. B., Sharma, V., Nunnery, C., Kang, B. B., and Dagon, D. (2007). Peer-to-peer botnets: overview and case study. *Proceedings of the first conference on Hot Topics in Understanding Botnets*.

Gu, G., Zhang, J., and Lee, W. (2008). BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*.

Kang, J. and Song, Y.-Z. (2010). Detecting new decentralized botnet based on kalman filter and multi-chart cusum amplification. In *NSWCTC 2010*, volume 1, pages 7–10.

Levy, E. (2004). Interface illusions. *Security Privacy, IEEE*, 2(6):66–69.

Liu, J., Xiao, Y., Ghaboosi, K., Deng, H., and Zhang, J. (2009). Botnet: classification, attacks, detection, tracing, and preventive measures. *EURASIP Journal on Wireless Communications and Networking*.

Mirkovic, J. and Reiher, P. (2004). A taxonomy of ddos attack and ddos defense mechanisms. *SIGCOMM Comput. Commun. Rev.*, 34(2):39–53.

Namestnikov, Y. (2009). The economics of botnets. Technical report, Securelist.

NVD (2010). Vulnerabilities in the last three years. Technical report, National Vulnerability Database.

Porras, P., Sadi, H., Yegneswaran, V., Porras, P., Sadi, H., and Yegneswaran, V. (2007). A multi-perspective analysis of the storm (peacomm) worm. Technical report, Cyber-TA Project Page.

Project, T. H. (2004). *Know your Enemy: Learning about Security Threats*. Addison Wesley Publishing, 2nd edition edition.

Stewart, J. (2004a). Bobax trojan analysis. Technical report, SecureWorks.

Stewart, J. (2004b). Bobax trojan analysis. Technical report, SecureWorks.

Stewart, J. (2004c). Phatbot trojan analysis. Technical report, SecureWorks.

Stewart, J. (2006). Spamthru trojan analysis. Technical report, SecureWorks.

Stewart, J. (2010). Zeus banking trojan report. Technical report, SecureWorks.

Weber, T. (2007). Criminals ’may overwhelm the web’. Technical report, BBC News.

Wilbur, K. C. and Zhu, Y. (2009). Click fraud. *Marketing Science*, 28:293–308.

Wilson, C. (2007). Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress. Technical report, CRS Report for Congress.