**Yadigar N. Imamverdiyev[1], Gulnara B. Garayeva[2]**
Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]yadigar@lan.ab.az, [2]qarayevagulnare@mail.ru
DOI: 10.25045/jpit.v09.i1.04

# MULTI-LEVEL ANALYSIS OF INITIATIVES IN COUNTERING BOTNETS

*Botnet is a network of infected with malware and remotely controlled computers. In recent years, rapid increase in the scale of botnets, their use in cybercrime purposes and tangible and intangible damages stemming from botnets demonstrate the importance of a comprehensive struggle with them. The paper studies directions, methods and stakeholders of fight against botnets and analyzes anti-botnet initiatives at international, national, social and individual levels.*

***Keywords:*** *botnet, cybersecurity, cyberspace, Internet Service Providers, anti-botnet initiatives.*

## Introduction

Botnets are the networks of infected computers with malicious programs (bots). This malware remotely infects computers and enable the botmaster to use them for their own hazardous and illegal purposes. These purposes include Distributed Denial of Service attacks (DDoS), spamming, information theft, and so forth. The number of infected computers and the damage caused characterize the extent of the botnet threat.

The rapid increase in the number of bots is due to the growth of broadband Internet services and the expansion of new fields in the development of malicious software, which enables the growth of criminal events. Damage caused by malicious programs is measured in millions of US dollars. This also proves the relevance of the fight against botnets. There are various approaches of combating bots from individual, social, economic, national, regional and international aspects [1]. Botnet-based cyberattacks against Estonia in 2007, Georgia in 2008, and Iran in 2009 once again proves the importance of combating botnets in terms of national security. This is directly related to the cyber security policy of the states [3].

Today, governments are relying on cyberspace in all areas - from financial transfers to military operations. Nevertheless, the Internet has not been developed for security, but for a high-speed data exchange. The target and extent of cybercrime in recent years have shown the importance of the international co-operation in this field.

There are stakeholders directly or indirectly participating in this or that level of combating botnets. These are legislative and law enforcement agencies, Internet providers, cyber security solutions vendors, research institutes and researchers, Internet consumers and end-users. Many international and national working groups have been established to combat botnets; advanced experience and recommendations have been developed; and the projects supported by legislation have been implemented. However, the botnet danger continues to grow every day. This is due to the huge revenue of the botnet economy and the fact that botnet managers are prosecuted in few cases [5].

Even though, the measures taken for the combat against botnets in most developed and developing countries of the world are increasing the confidence that the number of botnets will decline in the future.

## Key aspects of the fights against botnets

To determine the direction of anti-botnet measures, it is important to study the problems related to their condition [6]. The issues related to botnets are as follows:

*The exact determination of the actual number of existing botnets.* Thus, the figures mentioned on the number of real botnets are not exact and they are not scientifically justified. In addition, their number is not the only factor for the evaluation of the danger caused by the botnets.

*The importance of co-operation to evaluate the danger of botnets.* Remotely controllable and up-to-date malware programs also accelerate the geographical coverage of botnets. It is

therefore advisable to collaborate with geographical regions in different areas (such as information, practice and recommendation codes, etc.).

*Inadequacy of current legislation*. Various documents on cybercrime, adopted particularly by the European Union member states, enhance the effectiveness of the fight against botnets. Nevertheless, the current scale of botnets still indicates inadequacy of current legislation [7, 8].

In addition, the best solution for the global botnet is associated to the international cooperation between states, technical and regulatory agencies. For the effective development of the International collaboration strategy, a robust political support should be provided among the stakeholders. This includes reliable reports on attacks, substantial information about known threats, evidences and clues for the arrest of the cybercriminals, and so forth.

The fight against botnets has the following key trends [6]:

**1. Reducing the number and impact of existing botnets.** In order to reduce the number of botnets, it is important to provide the followings:

- unconditional support for infected computer owners at all stages of bot cleaning process;
- development of monitoring and detection of botnets, and malware analysis;
- extension of the efforts for botnets destruction;
- organization of information exchange between the stakeholders of the botnets reduction process;
- bringing the laws against cybercrime to the international level;
- extension of the process of botnets destruction until the entire botnet infrastructure is detected.

**2. Preventing new infections.** Prevention of new botnet infections is essential. This process includes the following measures:

- detecting botnets at the initial stage of the infection to reduce their spread;
- implementing the measures for public awareness;
- filling the gaps in operating systems;
- increasing the system security and so forth.

Botnet infection can be slowed down or completely prevented through the participation of software developers in the anti-botnet processes and user awareness.

**3. Reducing the revenue of botnets.** One of the reasons for using malicious software is the revenue. The counter-measures should be primarily aimed at reducing the revenue from cybercrime, particularly, from botnets. For this purpose, the following measures should be taken:

- prohibition of the use of malicious apps in the legislation;
- public awareness and so forth.

There are following factors affecting the hasty spread of botnets:

- easy and inexpensive infection of personal computers with malicious bot apps;
- quite attractive profit of botnet activity;
- low probability of penalties imposed on botmasters.

## Contributors to the fight against bots

There are parties involved in this process and directly or indirectly interested in the reduction and destruction of botnets [8]:

***1) Legislative and law enforcement agencies.*** Legislative and law enforcement agencies that form the cyber-security policy of the state have an important position in the fight against botnets. The responsibilities of the legislative agencies are as follows:

- modernizing an existing national legislation and establishing a practical basis for dealing with various aspects of cybercrime;
- adapting the present laws or adopting new ones to improve the botnets reduction and international co-operation;

– ensuring relationships that precisely define the responsibilities and roles established among member states within the framework of cooperation, and so forth.

***2) Vendors of cyber security solutions (antivirus companies, etc.).*** One of the stakeholders in the process of botnets reduction is software manufacturers, which provide prevention of botnet infections, including botnet balancing.

***3) Academic institutions (research institutes, etc.).*** Authorized research institutes provide more effective results in combating botnets. Developed detection methods should be an applicable tool for reducing complicated hazards and new threats. Publishing and disseminating research results should be organized by responsible agencies.

***4) Internet service providers (ISP).*** ISPs play the role of "key" in the identification and reduction of botnets. Many countries have ISP national fight initiatives. ISPs can often solve the following problems [9]:

– preventing end-users from infecting malicious software;
– enhancing civilian awareness on cyber security;
– ensuring easy access to information that is important for detection;
– informing end-users about remote controlled infections.

***5) Internet consumers and end users.*** End users are getting involved in this or that way at all levels of the fight against botnets. The users involved in the botnet spreading are becoming material and moral victims. Therefore, one of the key stakeholders in the reduction of botnets is the recent Internet consumers.

**Anti-botnet initiatives**

Anti-botnet problems need global (regional), national (state), social (social), economic and individual solutions.

***Global Fighting Initiatives***

Any global and regional disruptions of cyberspace are observed with the most severe consequences. Cyber cooperation, including political cooperation are important at the regional or global level. Thus, the regional stability of the cyber-infrastructure is based on the stability of the economic and political relations. The struggling mechanisms at this level should be formed by the international organizations, states, ICT-related stakeholders and others, and should guarantee the management of fighting any global intervention [10, 11].

Due to the increased global botnet threat, many collaborative initiatives have been launched at national and international levels, while existing organizations have intensified their activities in this area. The main objective of these organizations is to establish and maintain confident relationships between various organizations to accelerate the fight against botnets and to simplify the process of sharing critical information and knowledge, and to regulate authority among all parties.

The *Botnet Mitigation Toolkit* project proposed by *ITU (International Telecommunication Union)* in 2007 is the first international initiative to combat botnets [12]. This project generally characterizes the danger of botnet and provides recommendations for the problem solution at various levels as political, technical and social aspects:

- Political aspect supports the dissemination of the legislation on cybercrime and promotes co-operation among stakeholders, and ensures the balance between user privacy and security;
- Technical aspect specifies the role of Internet service providers for botnets' detection, control of domain name registrations and registers, financial institutions involved in the process of botnets' reduction;
- Finally, the social aspect ensures that users are more accessible by organizing the educational work and using visual media, as well as organizing the dissemination and periodic updating of security software.

Global standardization in the fight against bottlenecks is regulated by CYBEX (*Cybersecurity Information Exchange Framework)* [13]. The standard equally links various cyber security agencies and eliminates errors. Information on various stakeholders in the field of botnet detection is collected and structured. A unique object identifier is used to eliminate exchange barriers between organizations and provide easy access to services and resources.

***Voluntary working groups***

Voluntary working groups created by a number of organizations also play crucial role in the fight against botnets. One of such groups is *WPISP (Working Party on Information Security and Privacy)*, which was established in 2010 by *OECD (Organization for Economic Co-operation and Development*) [14]. The WPISP is an international exchange platform. The coverage of the group includes malicious apps, cyber security policy, and the protection of critical information infrastructure.

The group analyzes the role of ISPs in the botnet reduction and the role of states in the Internet stability and security enhancement. The international trainings organized by the groups and their public-private partnerships are promising.

The role of voluntary targeted workgroups involved in the destruction of hazardous botnets, such as Conficker, Mariposa and Waledac, should also be mentioned. Conficker Working Group, launched in 2008, frights against the botnet developed with malicious bot software. It has also managed the cooperation between several international institutions and organizations for more effective and coordinated countermeasures [15, 16].

Mariposa Working Group was created by the Information Security Center of the Georgia Institute of Technology, Panda Security, Neustar, Directi and several anonymous security researchers after the Mariposa botnet was discovered in May 2009 [17, 18]. Due to the activity and co-operation of this group, the botnet was crushed, and even botmasters and malicious bot apps developers were charged with the criminal responsibility.

Waledac Working Group, which combats the Waledac botnet under B49 operation, has discovered the botnet due to the collaboration between Mannheim University, Vienna University of Technology, Bonn and Washington Universities. The latest botnet crushes were implemented by the China National CERT (*Computer Emergency Response Team*).

***National anti-botnet initiatives***

At present, cyber security policies constitute security measures taken within the national borders. Unfortunately, many states have turned cyberspace into a real cyberwar venue, and do not hesitate to use the botnet opportunities. Consequently, international anti-botnet efforts are limited to just a few states or regions.

One of the most common conflicts in cyberspace is the cyber intervention along with the physical intervention into the critical infrastructure in any country, where the biggest problem is finding cybercriminals. This is even more challenging when it comes to real warfare and the use of botnet capabilities. This calls for the states to join the international security initiatives along with cyber-security policies [20, 21].

There are approaches that can be applied at the state level, which are effective enough in the fight against botnets. Germany, the Netherlands, Japan, South Korea, the USA, Australia, Brazil, Romania and other countries have the best experience in the fight against botnets.

***Germany***

German Anti-Botnet Assistance Bureau has been established with the cooperation and support of the *German Federal Office for Information Security Agency (BSI)* and the *Association of the German the Internet Industry* [22, 23]. The main goal of the Bureau is to remove Germany from the list of 10 most botnet creating countries. The project, which is currently in progress, is a model for many countries. Based on the ISP-based information, botnet cleaning process is

implemented in three stages:

1. Infected computers are indirectly identified by spamtraps or honeypots;
2. Users of the infected computers are warned by ISPs in different ways (e-mail, traditional mail, etc.). The warning contains general information about malicious apps, the links to the software needed for malware cleaning, and the confidential number;
3. Users can get additional interactive support by using the confidential number. In addition, the knowledge gained at this level is collected for the next experience.

The operational project is coordinating the rapidly growing ISPs, IT security and social networking services of Germany, however, the main problem is the laws of this country on the privacy and protection of personal information, which does not allow to monitor relationship at the content level. Detection technologies provided by only spam traps and "honeypot" are considered.

***The Netherlands***

In 2009, a new project to combat the botnets was developed due to the collaboration of 14 ISPs covering over 98% of the Dutch Internet market [24]. The project is based on the information exchange between the member ISPs and best practice codes. The project consists of customer warning system, support for combat methods, and cleaning of detected systems.

***Australia***

The Australian Communications and Media Agency launched the Australian Internet Security Initiative in 2005 to reduce the number of infected computers in the country [25, 26]. The initiative is based on the best practice code developed by the Australian CERT. Though the project is voluntary, since 2005, the number of ISPs has increased from 6 to 100. The main idea of the project is to increase the users' knowledge about malicious software and actions, to detect infected devices remotely and to inform the responsible network providers. The Internet access of the infected device is restricted by the network provider for the protection of user data and prevention of further damage. Then, the bot cleaning process is implemented through certain software. In addition, the state agencies responsible are reported for taking appropriate measures on suspicious circumstances.

***United States of America***

In 2012, the *US Communications Security, Reliability and Interoperability Council* launched the *US Anti-bot Code of Conduct for ISPs* to diminish the number of botnets [27]. The code specifies network security for more reliable online sharing and the collaboration between service providers and end-users, and the role of ISPs in this regard. To improve the effectiveness of the fight against bots, the code considers the collaboration between all the stakeholders on the Internet - antivirus and security vendors, software and hardware manufacturers, domain name registrars, end-users, IT departments, web-entrepreneurs, and so forth. The code is voluntary and defines the main tasks of participating ISPs as follows:

- ***Enlightenment***. Awareness of users about botnet threats and its protection ways;
- ***Detection***. Detection of bot activities at ISP level;
- ***Warning***. Informing users about infection or assumed infection;
- ***Cleaning***. Assisting or directly participating in bot cleaning from infected device users to clean bots this work;
- ***Collaboration***. Information exchange and periodic notifications with other participating ISPs.

***Japan***

In 2006, the Japanese *Cyber Clean Center (CCC)* was established, and is currently operating to combat botnets. The activities of the institution are supported at the state level, and it considers the cooperation with several institutions and organizations [28]. The center has joined more than 70 ISP projects that are responsible for approximately 90% of the Internet service in the country. The project participants are merged in three major groups:

- Telecommunication Information Exchange and Analysis Center responsible for the anti- bot system;
- JP-CERT (Japanese National CERT) responsible for analysis of bot apps;
- Information Technology Promotion Agency (IPA) responsible for enlightening users to avoid infection.

***South Korea***

*Korean Internet Security Agency (KISA)* and *Korean National CERT* launched Korean Anti-botnet campaign related to an increasing number of DDoS attacks and infected PC [29,30]. The approach consists of three main parts:

- Infected devices are detected with the use of specialized *DNS (Domain Name System)* that identifies suspicious requests and connections. More detailed information is acquired from the reports of malware analysis and intervention detection systems.
- KR CERT performs botnets detection and reduction using the central DNS management service. Domain names used for malicious purposes can be easily *sinkholed*. In this regard, domain names and IP addresses used for fraud through special *DNS Resource Records* are registered.
- To complete botnet reduction efforts, KR-CERT, ISPs, and IT-providers collaborate to inform and protect the infected users.

In addition, electronic call center (118) serves for the Internet-related security incidents.

***Brazil***

The Brazilian national CERT is implementing botnets reduction projects based on the experience of other countries. The projects provides joint collaboration among several ministries, IT agencies, ISPs, non-governmental organizations and academic institutions [31]. The main goal is to improve the security of cyber infrastructure, reduce botnet-based activities and botnets. The following three areas are mainly operating:

1) Collecting information about incidents (statistical data, support, etc.);
2) Organizing trainings and awareness activities (courses, documents, presentations, etc.);
3) Network monitoring (distributed honey-pot and spam-pot).

***Public (social) combatting initiatives***

The third level of cyber security solutions comprises the establishment of public relations against malicious activities on the Internet. Social engineering, which is one of the most widely used techniques today, has led to a decrease in trust among people, the spread of disinformation between social individuals or groups, and increased cyber-terrorism. Rapidly developing information and communication technologies increase the social relations and the number of identifiers' theft from social networks. Particularly, cultural, religious or ethnic attacks are realized in the social networks or platforms using botnet capabilities.

Social awareness campaigns, which cover wider scope, are of great significance for the improvement of cyber security at the social level using social platforms. In this regard, national and international partnerships of the states with private sector are crucial.

*European Public Private Partnership for Resilience (EP3R),* established by the European Commission in 2009 is one of such groups [32]. Its objective is to create a framework for

cooperation between government and private sector stakeholders.

***Combatting at individual level***

The ultimate level of cyber security solutions is an individual approach to computer users who are directly involved in the rise and spread of malicious activities. In many cyber attacks, individuals are involved as victims being exposed to the breach of confidentiality or completeness of their personal information, and accessibility problems. Specifically, users are misused at all stages of development and performance of botnets. Successful activities of cyber security solutions at other levels are impossible without implementing the promotion of individual awareness activities.

More than 90% of the botnet infection occurs due to the negligence of PC users and the lack of awareness about the infection methods, which turn these users into a "soldier" of the bot "troops". The users' awareness includes information about botnets, their threats, complications, user-level diagnostics, and so forth. Almost all mentioned international and national fighting efforts are attempting to take some measure at the individual level. However, all this is insufficient compared to the real situation in modern cyberspace, and there is a need for more individual awareness-raising activities. This should be one of the key aspects of the cyber security policies of the states.

***Common characteristic of the fight against bots***

To evaluate the effectiveness of anti-bot responses at different levels, the success criteria must firstly be determined. The following criteria are used to measure the quality of the fighting approach [6]:

1) Restriction rate of botnet and botmaster's access to C&C infrastructure;
2) Identification of the exact number of bots operated within a botnet is essential for the subsequent cleaning tasks;
3) Identification of botmaster's revenue source and, at best, prosecute bot creators and botnet customers for criminal offence.

The termination of botnet C&C center may be a major achievement for botnet reduction, nonetheless, it should be taken into consideration that the bots are still remaining infected. In this case, only botmaster’s access to the botnet is restricted. Hence, C&C server detection does not provide solution of the problem for infected devices.

Uncleaned devices infected with malicious bot applications can be subjected to new botnets. The evaluation of the success of botnet reduction attempts is directly related to the cleaning of infected devices. However, sometimes this is insufficient as the same device can be a part of several botnets.

Additionally, undetected or unterminated C&C server can lead to the development of a new botnet stronger than the previous one.

**Conclusion**

Although, almost all states legally prohibit the remote control of computer systems, this obligation is not followed in practice and remains only as a requirement. The increasing number of bots and bot-based activities proves a need for further intensification of existing approaches and the development of new ones. Long-term international activities can only be effectively achieved by: reducing the impact and number of existing botnets, preventing new infections, and reducing revenues from botnets.

**References**


1. Tiirmaa-Klaar H. Cyber security threats and responses at global, nation-state, industry and individual levels. Ceri SciencesPo. 2011, pp.1–10.
2. Schmidt A. At the boundaries of peer production: The organization of Internet security production in the cases of Estonia 2007 and Conficker // Telecommunications Policy, 2012, vol.36, no.6, pp.451–461.
3. Wilson C. Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress. Library of Congress Washington DC Congressional Research Service. 2008, 43 p.
4. Herzog S. Revisiting the Estonian cyber attacks: Digital threats and multinational responses // Journal of Strategic Security, 2011, vol.4, no.2, pp.49–60.
5. Tiirmaa-Klaar H., Gassen J., Gerhards-Padilla E., Martini P. Botnets, cybercrime and national security. Botnets. Springer London, 2013, pp.1–40.
6. Plohmann D., Gerhards-Padilla E., Leder F. Botnets: Detection, measurement, disinfection & defence. ENISA Report. 2011, 154 p.
7. Plohmann D., Gerhards-Padilla E., Leder F. 10 Hard questions on botnet mitigation. ENISA Report, 2011, 18 p.
8. Vihul L., Czosseck C., Ziolkowski K., Aasmann L., et al. Legal implications of countering botnets. Joint report from the NATO Cooperative Cyber Defence Centre of Excellence and the European Network and Information Security Agency (ENISA), 2012, 67 p.
9. Van Eeten M., Bauer J.M., Asghari H., Tabatabaie S., Rand D. The role of Internet Service Providers in botnet mitigation: an empirical analysis based on spam data / Workshop on the Economics of Information Security (WEIS), 2010, pp.1–31.
10. Sood A.K., Enbody R.J. Crimeware-as-a-service − survey of commoditized crimeware in the underground market // International Journal of Critical Infrastructure Protection, 2013, vol.6, no.1, pp.28–38.
11. Leder F., Werner T., Martini P. Proactive botnet countermeasures: an offensive approach. The Virtual Battlefield: Perspectives on cyber warfare. IoS Press. 2009, vol.3, pp.211–225.
12. ITU Botnet Mitigation Toolkit: Background Information. ITU Telecommunication Development Sector, ICT Applications and Cybersecurity Division, 2008, 78 p.
13. Rutkowski A., Kadobayashi Y., Furey I., Rajnovic D., Martin R., Takahashi T., Schultz C., Reid G., Schudel G., Hird M., Adegbite S. CYBEX: the cybersecurity information exchange framework (x.1500) // ACM SIGCOMM Computer Communication Review, 2010, vol.40, no.5, pp.59–64.
14. Pijpker J., Vranken H. The role of Internet Service Providers in botnet mitigation / European Intelligence and Security Informatics Conference, 2016, pp.24–31.
15. Nadji Y., Antonakakis M., Perdisci R., Dagon D., Lee W. Beheading hydras: performing effective botnet takedowns / Proc. of the ACM SIGSAC conference on Computer & communications security, 2013, pp.121–132.
16. Asghari H., Ciere M., Van Eeten M.J. Post-mortem of a zombie: Conficker cleanup after six years / Proc. of the 24th USENIX Security Symposium, 2015, pp.1–16.
17. Sully M., Thompson M. The deconstruction of the Mariposa botnet. Defence Intelligence. 2010, 32 p.
18. Sinha P., Boukhtouta A., Belarde V.H., Debbabi M. Insights from the analysis of the Mariposa botnet / Proc. of the 5th International Conference on Risks and Security of Internet and Systems (CRiSIS), 2010, pp.1–9.
19. Gold S. Taking down botnets // Network Security, 2011, vol.2011, no.5, pp.13–15.
20. Shirazi R. Botnet Takedown Initiatives: A Taxonomy and Performance Model // Technology Innovation Management Review, 2015, vol.5, no.1, pp.15–20.

21. Salles R., Gu G., Swimmer M. Editorial for Computer Networks special issue on ‘‘Botnet Activity: Analysis, Detection and Shutdown’’ // Computer Networks, 2013, vol.57, no.2, pp.375–377.
22. German Anti-Botnet Initiative. http://www.botfrei.de
23. Karge S. The German Anti-Botnet Initiative / OECD Workshop: The role of Internet intermediaries in advancing public policy objectives, 2011, pp.1–4.
24. Schless T., Vranken H. Counter botnet activities in the Netherlands: a study on organisation and effectiveness / Proc. of the 8th International Conference for Internet Technology and Secured Transactions (ICITST), 2013, pp.442–447.
25. Editors: “The Australian Internet Security Initiative – Internet triage in action?” // ACMAsphere Newsletter, 2010, Issue 51, pp.14–15.
26. The Australian Internet Security Initiative: Interviews with industry Participants. Australian Communications and Media Authority (ACMA) Report. October 2015, 62 p.
27. U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs): Barrier and Metric Considerations. The Communications Security, Reliability and Interoperability Council (CSRIC) Final Report, March 2013, 99 p.
28. Cyber Clean Center Japan. https://telecom-isac.jp/ccc/en_index.html
29. Krebs B. PCs Used in Korean DDoS Attacks May Self Destruct. Washington Post Security Fix Blog, 2009.
30. Information Security in Korea – “Safe Internet, Happy Future!”. Korea Internet Security Agency (KISA) Report, 2015, 55 p.
31. Opperman D. Internet Governance and Cybersecurity in Brazil. In book: Multilateral Security Governance. KAS Rio de Janeiro, 2014, pp.167–181.
32. Irion K. The governance of network and information security in the European Union: the European Public-Private Partnership for Resilience (EP3R). In book: The Secure Information Society. Springer London, 2013, pp.83–116.