



## Botnets: 10 Tough Questions



## ABOUT ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of expertise for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard for information on good practices. Moreover, the agency facilitates contacts between European institutions, the Member States, and private business and industry players. This work takes place in the context of ENISA's Emerging and Future Risk programme.

## CONTACT DETAILS

Editor: Dr. Giles Hogben giles.hogben [at] enisa.europa.eu  
Internet: <http://www.enisa.europa.eu>

Authors: Daniel Plohmann daniel.plohmann [at] fkie.fraunhofer.de  
Elmar Gerhards-Padilla elmar.gerhards-padilla [at] fkie.fraunhofer.de  
Felix Leder felix.leder [at] fkie.fraunhofer.de

### **Legal notice**

Notice must be taken that this publication represents the views and interpretations of the editor, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent the state-of-the-art in anti-botnet measures and it may be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2011

## LIST OF CONTRIBUTORS

This report is the result of a project group consisting of representatives from ENISA, Fraunhofer FKIE, Germany, and University of Bonn, Germany, using input and comments from a group selected for their expertise in the subject area, including industry, academic and government experts.

Angelo Dell'Aera	Security Reply
Pierre-Marc Bureau	ESET
Raoul Chiesa	@ Mediaservice.net
Christian Czosseck	Cooperative Cyber Defence Centre of Excellence
Christopher Elisan	Damballa, Inc.
Dennis Heinson	University Kassel/CASED
Vincent Hinderer	CERT-LEXSI
Ivo Ivanov	<a href="#">eco</a> - Association of the German Internet Industry
Vitaly Kamluk	Kaspersky Lab
Sven Karge	<a href="#">eco</a> - Association of the German Internet Industry
Tobias Knecht	<a href="#">abusix.org</a>
Matthew McGlashan	CERT Australia
Damian Menscher	Google
Jose Nazario	Arbor Networks
Mahmud Ab Rahman	MyCERT
Marco Riccardi	The Italian Honeynet Chapter and Barcelona Digital
Anna-Maria Talihärm	Cooperative Cyber Defence Centre of Excellence

*The above list contains only experts who have permitted publication of their contribution. The views expressed in this publication are those of the editor, unless stated otherwise, and do not necessarily reflect the opinions of the participating experts.*

## INTRODUCTION

As part of the project “Botnets: Detection, Measurement, Mitigation & Defence” a series of questions was discussed on an accompanying mailing list by internationally renowned experts in the field of botnets between September and November 2010. This document, composed by ENISA, Fraunhofer FKIE, Germany, and the University of Bonn, Germany, presents a selection of the most interesting results of the ongoing mailing list discussions.

### 1 HOW MUCH TRUST TO PUT IN PUBLISHED FIGURES?

Many numbers have been published regarding the threat posed by botnets and especially on their size in terms of infected machines. Most of these numbers are arrived at by extrapolation from a sample that represents just a small fraction of the total number of potential victims, obtained by counting unique IP addresses only. A good example of the inaccuracy of counting unique IP addresses alone is the work of Stone-Gross et al. on the Torpig botnet, who had the opportunity of evaluating a unique bot identifier used internally by the botnet against IP addresses. Their comparison of a ten-day period yielded a population of around 180,000 bots, when using the identifier, while counting unique IP addresses resulted in more than 1,200,000 infected hosts [1].

A common problem with extrapolated numbers is the lack of information about the exact methodology and corresponding time period of measurement. A positive example of how to handle this circumstance is the tracking information published by the non-profit organisation, Shadowserver Foundation [2]. Shadowserver tracks various activities related to botnets. For example, regarding command-and-control servers, a constant number of between 5000 and 6000 online servers were observed in the course of the year 2010. For the purpose of counting infected computers, three differently parameterised metrics are published, representing a simplified definition of a botnet threat level. This metric is defined as a counter that decreases over time, so long as no activity in the botnet is observed on a certain IP address. Every time the IP is active in the botnet, the counter is refreshed and set to its initial maximum value. Statistics are published for values of 5, 10, and 30 days respectively. A longer period clearly results in a higher bot count, as the chance increases that, during this time span, malicious activity connected with an IP address can be observed.

The accuracy of different measurement approaches is analysed in detail in [3] in chapter 3.

#### THE CASE FOR LACK OF ACCURACY

The degree to which botnet populations are **over** or under-estimated is hard to identify precisely, since both irregularities are provoked by opposing factors. Dynamic IP

address assignment and mobility of devices complicate exact size estimates by increasing “address churn” and hence intensifying the potential for exaggeration. On the other hand, hidden private networks, not directly accessible from the Internet, for example using network address translation (NAT), create a high potential for significant undercounting, which can also lead to inaccurate published numbers.

## HIGH INCENTIVE FOR EXAGGERATION

Media attention, publicity and interest in receiving financial support are strongly correlated with the level of threat published. Over the last few years, the term ‘threat level’ has been almost exclusively associated with the size of botnets. Well-known reported figures for botnet sizes that caught major media attention ranged from around 7-9 million bots for Conficker, over 13 million bots associated with Mariposa and up to 30 million infected machines in the Bredolab botnet. As big numbers imply big threats, therefore high attention, there is a significant incentive for overestimation.

In terms of DDoS, published data by potential victims of attacks is often not representative because they have an interest in protecting knowledge about their infrastructure and in not appearing to be “easy prey”. This can result in exaggerations of the attacker’s capacity, in order to deter further attackers from launching DDoS on them. Alternatively, information about unsuccessful attacks is seldom published, in order to avoid attracting attention or accidentally revealing information about their bandwidth capacity.

## TRANSPARENCY OF METHODOLOGY

If the methodology and time period considered are not clearly specified, one should not put much trust in the accuracy of the presented numbers. Even if the methodology and time period are specified, the numbers should be used carefully because of the aforementioned effects.

To get reliable size estimates at all, the botnet has to implement a mechanism for uniquely identifying bots, which is not the case for all botnets. Furthermore, the botnet operator might try to obfuscate the size of the botnet by disturbing the measurement.

A positive example of documentation is given by the Conficker Working Group in the context of up-to-date sinkhole data gathered by them [4]. They explain that the actual number of infections in comparison to their tracking results lies in the range of 25%-75% of the displayed value, which represents the potential maximum level of infections. At the time of writing, this suggests that the number of hosts infected with the Conficker malware is between 1,000,000 and 3,000,000. This large range represents the group’s aversion to quoting or stating accurate numbers for botnet populations [4].

## SIZE IS NOT EVERYTHING

The size of a botnet alone is an inappropriate and very inaccurate measure for assessing the threat posed by a certain botnet. For example, when considering Distributed Denial of Service attacks, the actual number of hosts participating in most DDoS attacks is in the hundreds [5]. Botnet size should be interpreted as a scaling factor for other, more specific metrics. For example if each bot has a certain bandwidth available then this bandwidth might be assumed to scale linearly with the number of bots (although this may depend on their global distribution).

## THREAT CHARACTERISATION IS STAKEHOLDER-DEPENDENT

The threat level posed by botnets should always be viewed from the perspective of the stakeholder in question. While providers of email services may be primarily interested in metrics related to spam generation by botnets, Internet Service Providers are interested in the identification of infected hosts on their networks in order to reduce the load of malicious traffic. Financial institutions are concerned about malware that has the functionality to support or carry out fraud as well as DDoS attacks. Governments have a desire to fortify their critical infrastructure against sabotage and DDoS, and also to protect classified documents and communication against threats like identity theft, which originate from specialised botnets.

It is therefore suggested that customised sets of metrics per botnet and stakeholder are used. A selection of possible metrics is presented in [3] in chapter 1.

## 2 WHAT ARE THE MAIN CHALLENGES ASSOCIATED WITH JURISDICTION?

The ability to take botnet countermeasures depends largely on the applicable body of law. In order to fight cybercrime effectively, there are several challenges to overcome. For example, some countries have still not ratified the Council of Europe Cybercrime Convention [6]. The objective of this Convention is to pursue a common criminal policy, especially by adopting appropriate legislation and fostering international co-operation. A more detailed discussion of these challenges is given in [7].

## STATUS OF IP ADDRESS AS PERSONAL DATA

One of the most widely discussed topics, when considering legal obstacles for botnet countermeasures, is the status of IP addresses as personal data. Jurisdictional differences in interpretation of this status are particularly critical of information sharing. IP addresses are the most important identifier, used by security researchers and ISPs alike, for computer systems connected to networks. To apply countermeasures more effectively against botnets, a practically-oriented strategy should be found [7] for balancing privacy and data protection laws, with the ability to investigate cybercrime, For example, allowing ISPs in Europe just to inspect traffic for target IP addresses,



where clear evidence can be provided of malicious activity, would already help identify infections on their customers' computers more effectively.

## CROSS-BORDER COORDINATION

Global cooperation is an indispensable condition for the successful investigation of botnets. Cross-border coordination is therefore a major challenge. It can only be negotiated through clear attribution of responsibilities and definition of interfaces between the parties involved.

In particular, the heterogeneity of legal situations in different countries suggests a need for the harmonisation of related laws. This would simplify cooperation and hand-over processes, as legal complexity would be significantly reduced. The plan to establish a European cybercrime centre by 2013 (cf. [8]) is a promising first step in improving cross-border coordination within the EU, and also from a global perspective.

## STANDARDISATION OF ROLES, RESPONSIBILITIES AND RIGHTS

In the fight against botnets, time is of the essence, and so there is a need for an acceleration of legal processes. To achieve this, roles, responsibilities, and finally rights of parties involved in the fight against botnets should be standardised, ideally at a global level. This includes their protocols of information exchange.

Clear roles should be defined and these roles should be granted specific rights. As an example, even though ISPs are apparently in a good position to monitor, detect, and therefore counter incidents and outbreaks, their freedom of action faces strong legal restrictions. The participation of all major ISPs in the German Anti-Botnet Initiative [9] indicates the general willingness of some major ISPs to support customers by notifying them if an infection has been clearly identified. However, this willingness is not the case with all ISPs, as it is connected with significant financial investment. Furthermore, the legal basis for fully effective remote detection of infections, e.g. through responsible and strongly limited traffic inspection, has not yet been established.

To support mitigation efforts, the installation of a "Good Samaritan Law" in the context of botnets should be examined. The idea behind this approach is to institute certain exceptions from liability in the case of individuals who choose to act against botnets (or other malicious software) with good intentions. This could reduce the hesitation towards analysing botnets shown by security researchers and other professionals. On the other hand, careful consideration would need to be given to provisions for preventing digital vigilantism.

### 3 WHAT SHOULD BE THE MAIN ROLE OF THE EU/NATIONAL GOVERNMENTS?

#### EU LEVEL

The main role of the EU should be the harmonisation of Member States' cybercrime legislations. This includes keeping the legal framework up to date and defining the minimum (and maximum) standards Member States are required to enforce. The EU can go further, by taking on the role of mediator for information exchange between various national institutions focusing on cybercrime.

This raises the requirement for a permanent central point of contact with permanent availability. This can accelerate the corresponding processes and assist their execution by, for example, advising on legal questions. The EU proposes to establish such a central point of contact in the form of the European cybercrime centre that will be established by 2013 (cf. [8]).

Creating additional incentives and providing funding for industry measures in botnet research and mitigation should be achieved through Public Private Partnerships, in order to strengthen the international network and cooperation between industry, academia and government.

#### NATIONAL LEVEL

At national level, the most important task for Member States is to adapt legislation and penal codes for future botnet activities. In order to be able to handle incidents effectively, the widening of national and locally-specialised CERT mandates seems appropriate. In addition, law enforcers and courts should be specifically trained and prepared for dealing with cases related to cybercrime [8]. This training and the building of competence are seen as critical by many experts.

As it is a nation's obligation to provide a productive environment for their citizens' to live in and for their economy to grow, increasing their awareness of, and education about, basic IT security topics can provide a good complement to efforts from the side of end-users.

Furthermore, Member States should prepare themselves to face botnets and malware that affect their national security interests, e.g. espionage or manipulation of critical infrastructure. In this case, the state is obliged to act and respond accordingly and should be prepared with a comprehensive security strategy. This includes the definition of escalation procedures in response to acts of aggression by nation states.



## 4 WHICH PARTIES SHOULD TAKE WHICH RESPONSIBILITIES?

Responsibility regarding botnets can be associated with different stakeholder groups. For example, governments want to provide a safe and productive environment for their citizens and economies. It is assumed that private end-users possess the majority of all infected machines [10]. ISPs are in a special position as a conduit for malicious traffic emanating from their customers' machines. In addition to the discussions in this section, more extensive recommendations are given in [3] in chapter 5.

### GOVERNMENT: CLARIFY AND HARMONISE LEGISLATION ACROSS BORDERS

In general, parties facing the threat of botnets fear legal actions when actively participating in mitigation efforts. It is less an issue of the law itself than a lack of clear interpretation of existing laws. Unfortunately, the most promising and dynamic mitigation approaches cause the most significant legal obstacles in gaining explicit permission to implement them.

Current best practice, after the discovery of a botnet and the identification of C&C servers, is to contact the responsible service or hosting providers to inform them about the operation of malicious services in their network. The consequence, if the service provider is cooperative, is a shutdown of the server or sinkholing of the domain name. In the case of a non-cooperative service provider, a court order can help achieve these goals.

Where aggressive countermeasures attack the botnet's C&C infrastructure, e.g. a DoS attack, a remote takeover of the C&C command channel or server instances, or execution of code on the infected machines, legislation either prohibits their application or is unclear.

Consequently, clear laws and guidelines are a necessary condition, if investigators and researchers are to concentrate on their task and face the minimum of obstacles from legislation, while maintaining the appropriate safeguards of citizens' rights and freedoms, national sovereignty and civil order, in both national and cross-border contexts. Issuing clear and consistent laws and guidelines is a matter for legislation, and so can only be dealt with by governments.

### END-USERS: KEEP SYSTEM CLEAN

The level of responsibility the end-user takes on has to be increased. The end-user should be encouraged to take more responsibility for keeping his/her system clean, as a failure to do so increases not only the risk to the user's own data but also to other users and enterprises. Clearly, this should be accompanied by better security education and the raising of end-users' awareness of the social consequences of a

lack of responsibility for computer security. The social responsibility aspect should be especially strongly emphasised in this context. The removal of malware can be a complex task for the average user; Users should therefore be supported by other parties [11].

Finally, the question arises as to whether an infected and remotely-controllable system eliminates users' exclusive ownership, and whether external measures should be permitted to disinfect the system in order to regain control for the user.

### (INTERNET) SERVICE PROVIDERS AND NETWORK OPERATORS

Of all the stakeholders, ISPs are probably the best positioned to support users in, at least, detecting infections and, optionally, disinfecting their systems. On the other hand, these activities have significant financial implications for the ISPs, and market pressure forces them to operate cost-effectively. Another concern regarding user notification is the so-called "shoot the messenger" problem. Although informing customers of their potential infection helps them, they might blame the provider for delivering the unwelcome message.

One contributing expert stated that, during a sinkholing operation against a botnet, their team encountered the following situation several times: Even if a list of IP address and timestamp pairs was provided to a network operator, they were often not able to identify the associated customer, because this data was either not logged or not easily retrievable from the log files. There are therefore network operators, or even ISPs, that do not fulfil the technical requirements of informing their customers about an infection, even though in the EU, according to [12], ISPs are obliged to store this information for 6 months to be compliant with Articles 5 and 6.

In order to ensure that it is economically feasible for ISPs to operate services supporting the disinfection of end-user machines for customers, their efforts should be supported through Public Private Partnerships, as for example in the German Anti-Botnet Initiative [9] or the European Public Private Partnership, EP3R [13]. If national disinfection initiatives, such as [9], prove effective, this best practice should be widened to the EU as a whole.

## 5 WHERE TO INVEST MONEY MOST EFFICIENTLY?

### EDUCATION AND RESEARCH

As a greater sense of responsibility should be encouraged in end-users for the security of their devices, investing in education about internet security seems to be a necessary condition in order to raise awareness, competence and a sense of civic responsibility

Obviously, since research on botnets is the key to analysing, understanding and finally mitigating botnets, not only should educational facilities be funded, but other

independent institutions, non-profit organisations and industry should also be carrying out research.

The development of tools, techniques and processes for the efficient analysis of, and defence against, botnets is an important part of the successful fight against cybercriminal activities, since the success of mitigating processes often depends on the time available for a botnet to spread and for operators to implement new defensive measures. Therefore, the development of tools and techniques should be accelerated with the help of financial support and efforts to improve coordination and cooperation.

### REWARD FOR REPORTING

Often, interesting or useful information on current botnet operations is published by individuals who are not associated with parties that officially investigate these threats.

One expert from a large anti-virus company suggested creating a central resource that allows users to submit such information and get a reward if the information leads to significant progress in investigations. This idea was based on this expert's experience in the past of "accidental" publications helping to gather significant intelligence on specific cybercrime operations or threats.

To ensure the quality and correctness of submissions, a ranking system that allows the rating of submissions should be introduced.

This approach can help to have resources included from a bigger community and benefit the coverage and response time for investigating threats. Comparable approaches are the bug-hunting programs of Mozilla.org [14] and Google Chrome [15].

### DIGITAL ADDIOPIZZO AND DDOS MITIGATION

Mutual assistance and pressure groups that are focused on the world of offline extortion, such as the "Addiopizzo" [16] movement in Sicily, Italy (freely translated as: "Good bye, racket"), may serve, by analogy, as a prototype against DDoS-related extortion. In Addiopizzo, more than 280 shopkeepers and 10,000 consumers united against the Mafia and agreed not to pay protection money. In return, the association, in partnership with public authorities, provides support in, for example, legal suits.

The principle of mutual and public assistance as a means of combating extortion can be generally transferred to small and medium enterprises (SMEs) that are targets of extortion from DDoS attacks. For example, a communal fund could be set up for use in covering legal expenses when prosecuting cybercriminals.

Alternatively, it might be a good idea to install sponsored cloud services at a national or international level to create a "bomb shelter" for SMEs. This approach has already been deployed as a "digital bunker" by South Korea, after they were the target of widespread DDoS attacks in 2009 [17].

## 6 WHAT ARE KEY INCENTIVES FOR COOPERATIVE INFORMATION SHARING?

Information about, and coming from, ongoing research, as well as the mitigation of botnets, is highly fragmented. Even though small groups produce innovative and successful results, information exchange is still largely conducted through academic publications. Acquiring a global picture on who is currently working on what particular topic is an almost impossible challenge, and so work is done many times over in parallel or even obstructively. The way to address this challenge is through more efficient information sharing.

### MUTUALLY BENEFICIAL

The primary requirement for encouraging effective information sharing is for it to be mutually beneficial for participants. Information exchange is necessary to organise ongoing work, as well as making the results available for the mutual benefit and simplification of exchange processes.

The main incentive for contributors to engage in information sharing is either to save costs or gain fast access to high-quality information that cannot be obtained through their own efforts. The most crucial task is therefore to save time and money for the participants by getting high-quality information to the right parties in a timely manner. Furthermore, the exchange of information can help to avoid compromising ongoing investigations, because actions can be coordinated. Additionally, investigations can be complemented by the results of others working on the same target, and so reduce duplicated work. Feedback from the receiver to the provider of shared information on the usefulness and results indicates that their work is valued and, as has been mentioned by many experts, can lead to improvements in further data exchanges.

## 7 WHAT ARE KEY CHALLENGES FOR COOPERATIVE INFORMATION SHARING?

While information sharing clearly plays a key role in the fight against the global threat of botnets, a number of challenges are associated with these efforts.

### TRUST

Sharing information and, in particular, sensitive data about ongoing investigations is affected by the requirement for varying levels of confidentiality, due to the obligations of institutions involved. For example, financial institutions are subject to specific regulations that limit their potential for sharing data. Another barrier to information sharing is the need to hide these activities from criminals. Generally, information sharing requires a high level of trust between the parties involved.

It is important to mention that trust must always be mutual. On the one hand, the source of information has to be trusted, mostly in terms of reliability regarding the data provided. This includes the integrity and accuracy of the data, the context of its history and interpretation and how the data was collected, as well as the format in which the data is provided to the receiver. On the other hand, the receiver must be trusted as well. A major concern is the fear that the provided data will be leaked, since it may contain sensitive information about the sharing organisation, such as information about infrastructure and defensive provisions, or other details that may lead to loss of reputation if the shared information is published. A general point made by many experts is that personal acquaintance in an information-sharing context is beneficial to productivity [18].

Since botnet research and mitigation are typically a cross-border activity, establishing trust on a global level is complex. The idea of a centralised approach is discussed in section 9, including those aspects that are missing in the fight against botnets.

## DATA ORGANIZATION

The most crucial requirement is to get high-quality data to the right parties quickly, and tailored to their needs. To achieve this, the data needs to be organised in a way that is easy for the receiver to interpret, and to extract the relevant results or details in a timely fashion. Good practice involves (automated) discarding of duplicates, the use of common data interchange formats such as MMDEF [19], IODEF [20], MAEC [21], or ARF [22] / X-ARF [23], and metadata on how, when and by whom the data was collected.

Moreover, a key requirement, strongly emphasised by ISP representatives, is the accuracy of shared information, as errors can cause disastrous effects while incidents are being investigated or infections reported back to customers.

## INFORMATION AS PRODUCT

From an economic point of view, especially for small companies, exclusive information is often interpreted as a business asset. Against botnets, professional ethics have to be strengthened and commercial competition should be set aside in order to contribute to the fight against a common enemy. Where possible, information should be shared in a form that is devoid of commercial value, while still being useful in combating botnets (e.g. removing commercially sensitive information from logs).

## LEGAL ISSUES

Legal aspects and privacy issues play a decisive role in information sharing. The root cause of this is the general consideration of the privacy of communication versus the protection of users from threats. Contributing experts broadly agree that a meaningful balance has to be created, one that does not hinder investigations but still respects privacy. Current best practice consists of using passive mechanisms, like passive

honeypots (cf. [3], section 3.1.6), that need to be actively attacked. This way, malicious traffic originates directly from the compromised computers (only) to the detection mechanism, and no active interference with benign traffic is necessary for identification.

Implementation of the law is typically governed at a national level, which has led to a heterogeneous landscape of legislation on cybercrime across Europe. In order to facilitate global cooperation, these laws and their interpretation should be harmonised as quickly as possible, as suggested in [24]. Where differences exist, these should be made transparent in order to make cross-border botnet defence easier to execute. Moreover, any harmonisation efforts should consider the use of both minimum and maximum standards. This is because, even in the presence of an EU-wide minimum standard, such as that put into place by the 95/46 directive on data protection, extra provisions instituted by individual member states (which exceed the minimum standards) can have a significant effect on the practicality of cross-border defensive actions. In any such discussion, national sovereignty and the subsidiarity principle must, however, remain prime concerns.

In general, it should be noted that, in contrast to, for example, ISPs and law enforcers, botnet operators do not care about legal compliance. This leads to botnet operators being more dynamically organised and able to coordinate their actions more efficiently (especially faster) than those who counter them. The effects of the legal aspects of botnet countermeasures are analysed in more detail in [7].

## 8 ARE THERE UNSEEN/UNDETECTED BOTNETS?

Actual infection incidents and corresponding samples still serve as one of the most important sources for the detection and analysis of unknown botnets. But botnet developers work on anti-forensic techniques (countermeasures against investigation) and try to evade well-known detection methods. Consequently, botnets with robust defence techniques are able to stay undetected for long periods and also to delay investigation processes.

### LARGE NUMBER OF UNDETECTED BOTNETS

According to the experts consulted, it is likely that a significant number of botnets are unknown and untracked. Reasons for this include:

- Botnet activity that is not detectable by existing methods (as evidenced in some cases by subsequent identification).
- Frequent reconfiguration of bot-to-botnet memberships, leading to botnets with individually short lifespans but a great overlap in population.
- Frequent migration of command-and-control infrastructure, causing constant evasion of tracking.



As an example, server-side polymorphism, in combination with access restriction performed by the server, is an example of strong means against generic detection methods, causing serious problems for investigators.

## 9 WHICH ASPECTS ARE STILL MISSING IN THE FIGHT AGAINST BOTNETS?

### CENTRALISED COLLABORATION OR INFORMATION HUBS

In order to support worldwide collaboration, tools, mechanisms and procedures for sharing data that is related to incidents and ongoing investigations should be installed, or created where it does not exist. Experts emphasise that a central information sharing point, or a number of hubs, would have to provide a significant improvement in most of the processes involved in the fight against botnets in order to justify the possible overhead in efforts, and to be broadly accepted.

Obviously, a centralised approach requires concessions from all parties involved, since the corresponding benefit is not necessarily uniform. Therefore, for parties that tend to create more benefit to others than they may receive through the information-sharing process, appropriate incentives should be created to compensate their efforts.

Probably the most important benefit created by a central information-sharing service is the aggregation of insights into ongoing processes and the avoidance of mutually compromising activities.

The central practical question regarding the implementation of a central information-sharing system is: Which international body or country will lead the administration of the system and how will funding be organised? General challenges may arise from the variety of involved parties, e.g. through political and cultural differences that may lead to a reluctance to use the information sharing system. From a technical point of view, the integrity and confidentiality of data have to be ensured with respect to data classification systems. For example, access to shared information has to be managed with strong authentication mechanisms. Furthermore, ownership and localisation of shared data, as well as exchange protocols, must be agreed upon.

In the expert discussions a view was expressed that an independent organisation in the European (e.g. ENISA, Europol) or global context (e.g. UN, Interpol, NATO) could take the role of a central clearing house [8]. However, it was also stated that pilot projects of this approach were not accepted in practice, e.g. by a group of German ISPs who had tested central sharing of incident data. In this case, direct information exchange between affected parties was favoured over a central institution. The reason for this was mainly to limit the overhead created by this mode of operation.

Even without central data storage, an institution that enables faster communication between all parties involved is beneficial in the fight against botnets.

## SPEED UP LEGAL PROCEDURES

Clear global laws on cybercrime still appear to be the most important missing element in the effort needed to fight botnets efficiently. This includes rapid clarification of the legality of using technical tools, since the legal situation in particular countries slows down the development process of these tools, even though they play a decisive role in analysing and finally mitigating botnets.

Furthermore, the application of rules for dealing with emergency cases, where the justification for immediate action is obtained *ex post facto* should be examined. This would help to grant mitigation efforts the necessary reaction time to counter the highly dynamic characteristics of botnets.

## MORE EFFICIENT ANALYSIS TOOLS

Although a variety of approaches and tools for the analysis of malware specimens and botnets exist, further development is important. For example the time taken by Conficker's and Stuxnet's analysis, which in both cases took several weeks, is still clearly too long to allow a timely response to critical threats.

New techniques that allow more rapid classification and analysis of malware specimens are needed and should be supported by funding research institutions.

Additionally, new approaches to estimating the threat posed by botnets should be studied. For example, measures that include the potential impact of botnets on financial damage resulting from spam-sending capabilities, the sophistication of information theft and fraud mechanisms, and DDoS functionality (cp. [3], section 1.2.3 Attack Potential and Threat Characterisation).

## 10 WHAT ARE FUTURE TRENDS?

When analysing the development of cybercrime and botnets in particular, we can expect to see some of the following trends (a more extensive list of potential trends in botnets is given in [3] in chapter 6):

- The motivation behind attacks will increase further. We face economically and politically motivated attacks, as well as attacks aimed at gaining publicity.
- The quality and simplicity of available tools and development kits for attacks will continue to increase, so that increasingly non-expert attackers may cause severe damage.
- Concepts of command-and-control infrastructures used for botnets will adopt emerging technologies in order to achieve higher levels of deception and resilience. This involves network protocols and web standards, as well as new trends in real-time communication schemes or social networks for transmitting and disguising malicious traffic.

- Cybercrime has become a profitable business and heterogeneous legal situations complicate mitigation. This means that even not very complex botnets will last for long periods and be available for attacks and fraud.
- With the wide distribution of smartphones and the first bots for smartphones available, botnets based on smartphones and other new means of accessing the internet will add another dimension to the overall botnet threat.

With even unsophisticated botnets persisting for long periods, new kinds of botnets evolving and manifold motivations for attacks, it has to be expected that the number and severity of attacks will increase in the next few years.

## REFERENCES

- [1] Your botnet is my botnet: analysis of a botnet takeover. Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C., Vigna, G. In: Proceedings of the 16<sup>th</sup> ACM conference on Computer and communications security (CCS '09), 2009.
- [2] ShadowServer Foundation. [Online] <http://www.shadowserver.org>
- [3] Botnets – Detection, Measurement, Mitigation & Defence. ENISA report, 2011.
- [4] Conficker Working Group [Online] <http://www.confickerworkinggroup.org>
- [5] The Internet goes to War. Labovitz, C. Arbor Networks Security Blog, 2010. [Online] <http://asert.arbornetworks.com/2010/12/the-internet-goes-to-war>
- [6] Convention on Cybercrime. CETS No.: 185. Council of Europe, 2001.
- [7] The legal perspective on botnets. ENISA, to appear, Q2 2011.
- [8] “The EU Internal Security Strategy in Action: Five Steps towards a more secure Europe”, [http://ec.europa.eu/commission\\_2010-2014/malmstrom/archive/internal\\_security\\_strategy\\_in\\_action\\_en.pdf](http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf)
- [9] German Anti-Botnet Initiative [Online] <http://www.botfrei.de>
- [10] The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam (Data DSTI/DOC(2010)5). Van Eeten, M., Bauer, J. M., Asghari, H., Tabatabaie, S. STI Working Paper Series of OECD Directorate for Science, technology and Industry, 2010.
- [11] Might Governments Clean up Malware? Clayton, R. In: Proceedings of the 9<sup>th</sup> Workshop on the Economics of Information Security (WEIS 2010), 2010.
- [12] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications

networks and amending Directive 2002/58/EC. European Parliament and European Council, 2006.

[13] Non-Paper on the Establishment of a European Public-Private Partnership for Resilience (EP3R). EP3R Workshop, 2010.

[14] Mozilla.org - Bug hunting. Mozilla Community, 2010. [Online]  
[http://guides.mozilla.org/Bug\\_hunting](http://guides.mozilla.org/Bug_hunting)

[15] Encouraging More Chromium Security Research. The Chromium Blog, 2010.  
[Online] <http://blog.chromium.org/2010/01/encouraging-more-chromium-security.html>

[16] Comitato Addiopizzo. [Online] <http://www.addiopizzo.org/>

[17] Korea attacks force DDoS bunker creation. ZDNet, 2010. [Online]  
<http://www.zdnet.com.au/korea-attacks-force-ddos-bunker-creation-339307357.htm>

[18] Public Private Partnership in the Cybercrime Information Exchange. Brochure of NICC: United against cybercrime, 2008.

[19] IEEE Industry Connections Security Group [Online]  
<http://standards.ieee.org/develop/indconn/icsg/>

[20] RFC 5070 - The Incident Object Description Exchange Format (IODEF), 2007.

[21] Malware Attribute Enumeration and Characterization (MAEC) - A Standard Language for Attribute-Based Malware Characterization. [Online] <http://maec.mitre.org>

[22] RFC 5965 - An Extensible Format for Email Feedback Reports (ARF), 2010.

[23] X-ARF: Network Abuse Reporting 2.0 [Online] <http://www.x-arf.org>

[24] Proposal for a Directive on attacks against information systems, repealing Framework Decision 2005/222/JHA. MEMO/10/463, 2010.