

An Usage-Centric Botnet Taxonomy

Christian Czosseck and Karlis Podins

Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

Christian.Czosseck@ccdcoe.org

Karlis.Podins@ccdcoe.org

Abstract: Botnets have been a recognized threat to computer security for several years. On the timeline of malware development, they can be seen as the latest evolutionary step. Criminals have taken advantage of this new technology and cyber crime has grown to become a serious and sophisticated problem which law enforcement still finds difficult to deal with. In the past few years we are witnessing a movement away from cyber crime. Nation states become the target of attacks as well as actively using botnets to project their own power in the political or military domain. To study the new and emerging cases of botnet usage we propose an usage-centric botnet taxonomy. Although there are already a number of botnet taxonomies published, most of them have a technical viewpoint and often consider cyber crime as the major driver to use botnets. While it may be true for now, we believe that such approach might not be holistic enough to describe the current and future developments. Besides the trend of specialized botnets being developed, the number of botnet users is increasing, with new motivations coming along. The taxonomy proposed in this paper takes a different viewpoint by focusing less on technical attributes than on the actors using botnets and the functionality requested by them. Major difference from existing research is that proposed taxonomy classifies instances of botnet use. Based on existing taxonomies, case studies of recent botnet incidents and cyber warfare doctrines of selected nation-states, we explore theoretical and already seen ways of botnet usage. We propose new classification of botnets based on their technological attributes, the users and the intended effects on the target to provide a holistic picture of the current situation. We also test the proposed taxonomy on seven instances of botnet use.

Keywords: botnets, taxonomy, incident categorization

1. Introduction

Botnets, large numbers of remote controlled computers distributed all over the Internet and centrally controlled by so-called botmasters, are a persistent and continuously evolving threat to the Internet community, always seeming to be one step ahead of countermeasures and take-down attempts. Over the last years we have seen more and more sophisticated botnets, improving in multiple aspects like size, resistance to countermeasures and ways of spreading. A whole underground economy developed around botnets (Klein et al. 2011). More and more botnets have become a service offered by knowledgeable malware developers, ready to be rented out to everyone willing to pay (Schwartz 2010; Mills 2009). Besides technological evolution, the number of players as well as their motivations to use botnets is increasing. The recent history has witnessed several incidents where botnets were not used for financial benefit, but to deliver a political message, to conduct espionage or as an instrument for sabotage. The increasing diversity of botnet incidents requires for a structured botnet classification.

The usage-centric botnet taxonomy presented in this paper is designed to classify botnet events by means of usage, not botnets per se. By this our approach differs from other published taxonomies on botnets, which mostly focus on technical aspects.

The rest of this paper is structured as following: In section 2 we give an overview on related work of botnet taxonomies, motivating the uniqueness of our taxonomy; it will be described in the following section 3. We test the performance of the proposed taxonomy in Section 4 by categorizing a selection of recent botnet incidents according to it. Finally the conclusions and a discussion of future work are provided in Section 5.

2. Related work

Technical details of botnets and their highly visible functionality like DDoS attacks are well studied in scientific literature. But strategic aspects like motivation are rarely covered. (Weaver et al. 2003) present the *Taxonomy of Computer Worms*. They introduced *payload* and *motivation* attributes similar to the *functionality* and *motivation* attribute presented in this paper's taxonomy. (Weaver et al. 2003) present a more fine-grained classification in their features. On the other hand we separate users from their motivation, being combined to one in (Weaver et al. 2003). They also do not consider self-infection.

Detailed technical-level taxonomy of attacks and thorough literature review of technical-level taxonomies is given by (Hansman & Hunt 2005).

A technical defense-centric taxonomy of computer attacks is given in (Killourhy et al. 2004), where the authors discuss network level attack detection and classification. Several attack types like Denial of Service and Surveillance/Probing (corresponds to Information theft in the proposed taxonomy) are discussed in (Lippmann et al. 1998). (Distributed) Denial-of-Service (DDoS/DoS) attacks have been studied by (Lau et. al, Distributed Denial of Service Attacks). (Wun et al. 2007; Asosheh & Ramezani 2008; Wood & Stankovic 2004) offer taxonomies not limited to DDoS as such but covering architectural aspects of botnets like command-and-control structures or spreading strategies. Taxonomies of DoS attacks and countermeasures against them have been presented by (Champagne & Lee 2006; Mirkovic & Reiher 2004). A more detailed description of botnets internals including a comprehensive list of way how to use botnets several kinds of botnet usage) is presented by (Bacher et al. 2005; Barford & Yegneswaran 2007)The fast flux functionality provided by some botnets is covered in (Holz et al. 2008) and (Jose Nazario & Holz 2008).

Majority of research has considered botnets as collections of machines which are infected without the knowledge or consent of the respective owners (Klein et al. 2011). Recently in a small number of politically-tainted incidents botnet software has been installed intentionally by the owners (Ottis 2008; Panda Security 2010).

3. A usage-centric botnet taxonomy

Following the criteria for an effective taxonomy as introduced in (Killourhy et al. 2004), our taxonomy was designed to follow the principles of be *mutual exclusiveness*, *exhaustiveness* and *replicability* providing an instrument to classify botnet incidents of the past but also to deal with upcoming events. It consists of four features: 1. Users of botnets, 2. Motivations of botnet usage, 3. Functionality applied, and 4. Way of infection. A complete overview is provided in figure 1.

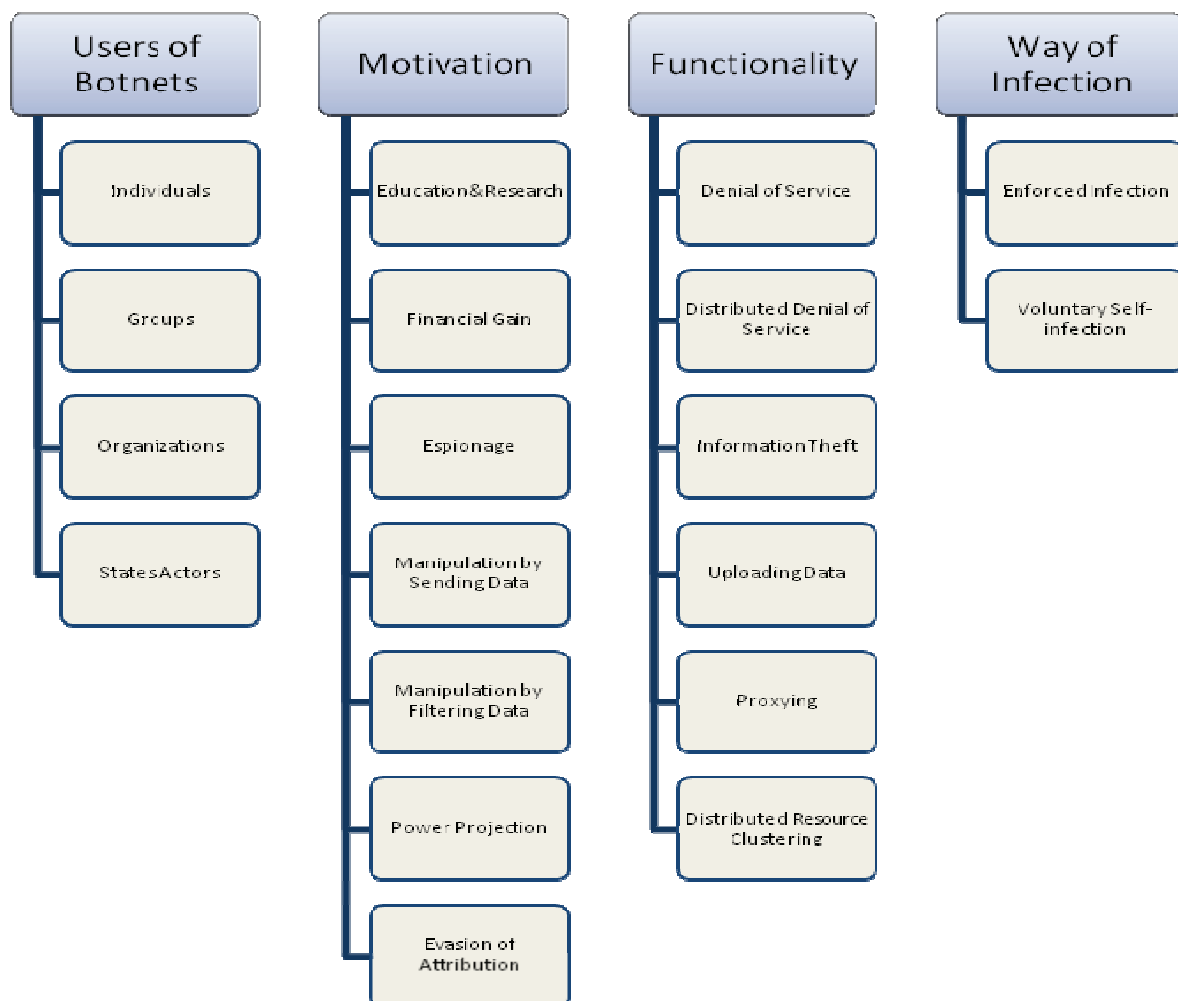


Figure 1: Usage-centric Botnet taxonomy

3.1 Users of botnets

Over the past years, developing and using botnets have become a profitable business. A well developed underground economy, providing botnet technology and services to everyone who pays (Mills 2009). The easy access to botnets introduces new players and motivations to appear. The first attribute of this taxonomy covers the user of the botnet and is motivated by a legal viewpoint considering who could be held liable for the action done.

Exclusion of middlemen

Over the time it has been witnessed that the underground economy has changed to a new service-oriented model, offering botnets for rent (Schwartz 2010; Mills 2009). This way a third party besides botnet user and the target gets involved. While these servicemen are important players, our taxonomy focuses on the perpetrator only. *We disregard the involvement of middlemen in the incidents, although they might be held responsible for the damages caused.*

Individuals are private persons using botnets independently.. This includes private persons using botnets for financial gain, education or out of curiosity. But also those, who want to express their opinion with digital force or support a political or ideological activity e.g. patriotic hacking, as in the case of the cyber attacks against Estonia in 2007 (Ottis 2008) or participants in the Operation Payback (Correll 2010). From a legal viewpoint, it is the individual who could be made responsible.

Groups shall cover all forms of collaborative and coordinated, but still loose group of individuals. It does not include groups formed based on a legal person (e.g. a company), and as such leaves only every single individual as being responsible for their actions. Persons with different roles might face different consequences, though. This covers examples where a group of persons were acting as a whole and out of internal motivation, as seen to a certain part in the Operation Payback incident with regards to the role of *Anonymous* (Panda Security 2010) and the later founded *AnonOps* (AnonOps 2010).

Groups also include examples of organized crime organizations, which do not use a legal body as a facade.

Organizations, in contrast to groups, are mainly defined by the legal person representing them. Beside of the individuals within the organization (and their personal liability), there is a legal person according to private law, which can be made responsible. This covers all companies using botnets for e.g. getting an (economic) advantage over another party, and to a limited extent on organized crime, if they also use a legal person for conduction at least parts of their operations. This class shall also include organizations established under international, private law.

State Actors are the type of users this taxonomy defines, and shall cover all organizations established under public national or international law. These include esp. parts of the executive power of a state, like police, military or intelligence services.

3.2 Motivations for botnet usage

Botnets are powerful and flexible tools providing their user with wide variety of functionality. While many different features of the botnet can be used at the same time, they are connected by the single motivation of the perpetrator at the time of usage. The second attribute provides the following broad classes of motivation behind botnet usage, which are similar to Motivations and Attackers identified by (Weaver et al. 2003).

Education & Research covers all activities done for the sake of getting familiar with the botnets, independently if one is interested in using, developing, analyzing or defending against botnets. The key attribute for this taxon is absence of a clear target e.g. violate somebody's rights or property.

Seeking *Financial Gain* is maybe the most common motivation for using botnets nowadays. This includes most cases of *information theft*, like stealing bank or credit cards information or license keys, as this information will be monetized nearly immediately by either using or selling it.

Espionage covers all cases where stolen information is not intended to be turned into money directly or at all. Instead, the gathered knowledge is used to influence own decisions, the relationship between parties

or to enhance an own situation awareness. This taxon is independent from the *User of the Botnet* as defined in the previous section and as such covers e.g. cases of state spying or industrial espionage.

The *Manipulation by Sending Data* is an umbrella class for all cases of botnet usage, where an outward directed data flow (from the viewpoint of the infected machine) is used a) to expression one owns opinion on something; or b) to manipulate someone other's opinion by sending wrong or misleading information.

The first sub-category covers cases like *hacktivism* (Denning 2001; Ottis 2008), where groups of persons use botnets to attack others, e.g. disturbing normal functionality of provided services, to support their political message. The second sub-attribute covers cases of propaganda or manipulation of services or outcomes of polls or voting, leading to a wrong final picture for others (Temmingh & Geers 2009a).

On the other hand *Manipulation by Filtering Data* shall cover all cases where denying access to information is the main reason for the botnet usage. This covers cases of censorship (see e.g. the Belarus case in Pavlyuchenko 2009), information blockages or redirection.

Botnets can be used as an instrument to *Project Power* in cyber space. To adopt Clausewitz freely, botnets can be used as a tool to influence another party's behavior or policy, after non-violent options are exhausted. This shall include, but not be limited to cases where botnets became part of *military operations* (e.g. the InfoOp against Georgia friendly news portals and governmental websites described in J. Nazario, 2009), or could be used to damage another's economy (Lemay et al. 2010). We also include cases of *sabotage* (like in the case of Stuxnet, see Falliere et al. 2010), or blackmailing (Sophos 2006) to be included here. It needs to be stressed here, that this taxon is independent from the user of botnets and as such reaches from individuals to state actors.

To *Evade Attribution* is one other reason one might want to consider using botnets. The mostly global distribution of botnets allows the user to let its victim believe that someone else was behind the cyber attack. This can even be extended to the intention to run a *false flag operation*. While botnets are not the only possible way to reach this goal, it is for sure a convenient one. As transnational cooperation in fighting cyber crime is still not developed globally, and not all nation states enjoy friendly relationships, disguising one real location and identity can be the reason to use botnets. Another scenario included is the (massive, distributed) *acquisition of resources*. Here the availability of the sheer number of zombies in the botnets, and with it the combined CPU processing power or storage capacity is used to set up a distributed service, there any single node does not have enough knowledge so that even if forensically analyzed, the service as a whole is not endangered or compromised.

3.3 Functionality

The functionality provided by a botnet is highly dependent on the developer of the botnet and can vary quite significantly between botnets. A fundamental feature of all botnets is the ability to remotely control computers and the ability to send files to them, e.g. for updating the bot client later on. On top of this a variety of different functions has been developed and became part of many botnets, while not all share always the same features. As of the common update feature, enhancing a botnet's capabilities later on is most often possible.

The third attribute of this taxonomy provides a set of generic features botnets might have. It combines features already seen in botnets over the past years, and also some new ones, the authors believe them to be reasonable to consider as they might been seen in the near future.. While this list has been prepared with care, based among others on (Weaver et al. 2003; Bacher et al. 2005), this is not claimed to be complete. The future might show new functionality not thought of till now.

Denial of Service (DoS) is the ability to disrupt the normal functionality *of the infected machine* as a whole. This enables the botnet master to shut down or even damage the infected system, making a recovery at least difficult.

Distributed Denial of Service (DDoS) is a functionality whereby a large number of service requests are directed to a target system, exhausting its available resources to especially answer to desired requests. For these attacks, the number of used botnet clients is the main criteria for the success of the DDoS, while is recognized that more sophisticated attack techniques might lead to a lower number of necessary bots to attack the target.

Information theft of data stored or processed on the infected machine or traffic passing or reaching it is another commonly seen functionality of botnets (Klein et al. 2011). This includes but not limited to the search for specific files, passwords or other sensitive data stored or typed into the infected workstation, e.g. banking credentials.

Uploading data, as the opposite of information theft, enables the botnet owner to deliver any desired file onto the infected machine. A basic implementation of this functionality is most often standard for all botnets, as it is necessary to *update* the installed malware. Beside this, the installation of additional software, e.g. further spyware, advertisement add-ons, or Browser Helper Objects is frequently seen (Bacher et al. 2005). In a bigger scale this could be used to implement a regional surveillance system (see e.g. the idea presented in Husted & Myers 2010).

But the botnet owner is not limited to, as he can basically upload any file he wants to the infected machine, and as such could e.g. place compromising or illegal data. Another special case of this taxon is the use of the botnet as a launch platform for other malware, accelerating its spreading by magnitude or enables regional targeted distribution of it like in the case of Stuxnet (Falliere et al. 2010).

This also includes the manipulation of existing files on the infected system to change their intended functionality. It is e.g. not uncommon for malware to disable running AV software or restricting access to AV websites (Porras et al. 2009).

Proxying is the ability to use the infected clients to execute actions on behalf of the botnet master, without him being revealed directly. Known cases are *Spam campaigns*, where the bots are tasked to send massively emails to a target group. Using a limited number of bots to form a *proxy chain* can provide functionality similar to anonymization services like the TOR network, where tracking traffic routes is close to impossible. Or they are used to hide the real location of some critical services, like phishing site or C&C servers, by implementing *fast-flux domains* (Jose Nazario & Holz 2008). Another not often seen way of using this functionality would be the *manipulation of voting* (Temmingh & Geers 2009b) or *click-based (advertisement) services* (Bacher et al. 2005).

Distributed resource clustering is a newly introduced function not commonly used so far. But the authors believe that there is room for botnet herders to explore this area more. It is understood that all the other mentioned functions also use resources of the infected machine to execute the mission they are tasked with. This taxon of botnet usage assumes the botnet herder to combine the available resources, namely CPU time or HDD space to build a service like known from the domain of clustered computing or cloud computing. The resource made available this way would enable him e.g. to conduct distributed calculations which could be useful for password cracking or to set up a distributed storage, where any member of the botnet holds part of the data the botnet herder wants to store. If designed well he could store huge amount of data, redundant and segmented in the botnet without any single bot client having enough parts for reconstruction a complete picture.

3.4 Way of infection

Enforced Infection:

Most botnets usually behave like any other malware trying to infect as many hosts as possible, spreading autonomously if ordered to do so. Computers are infected and join botnets without the knowledge or consent of the owner. Malware developers are actively developing and looking for new exploits to infect new hosts, and so far they are quite successful (Klein et al. 2011)

Voluntary Self-infection:

Besides the mentioned common way of infection, there have been a number of cases when owners voluntarily infected their machines to join a botnet. By doing that they supported a certain (politically motivated) cause, e.g. incidents in Estonia 2007 and Operation Payback 2010 (Ottis 2008; Panda Security 2010).

4. Application of the taxonomy

In order to test how well the taxonomy classifies events of botnet usage, we look at a selection of recent incidents involving botnets. These events are chosen to represent a wide variety of botnet uses; their or-

der does not reflect any sort order of importance. In some cases, several closely-related incidents are classified together as a group, because different events using the same bots happened at the same time. An overview is presented in Table 1.

4.1 Stuxnet

Although the number of Stuxnet infected hosts was small and spreading was highly targeted, the most basic features of botnets being the existence of a command and control capability support to consider Stuxnet as a botnet. (Falliere et al. 2010)

While categorizing this incident using the proposed taxonomy, the lack of trustworthy, full information left the attribute of Users of Botnets hard to decide. While there are many speculations on this, we decided to assume at least one *state actor* being involved. The Motivation is covered by the *power projection* taxon including sabotage, which seems to be the most likely motivation behind this incident. Stuxnet spread by involuntary infection, and its manipulation and damaging industrial systems represents a *denial of service* functionality.

4.2 GhostNet

There is no evidence on who are the players behind GhostNet. Speculations reach from (groups of) individuals up to state actors. As such we leave the user as *unknown*. But the small number of infected hosts (around 1300) and percentage of high-value targets (up to 30% of infected hosts belonged to ministries of foreign affairs, embassies, international organizations etc.) indicate that the motivation was espionage against pro-Tibet community. In order to do that, GhostNet was performing information theft from involuntary infected machines. (Deibert et al. 2009)

4.3 Operation payback

The *Operation Payback* was launched by a *group* of WikiLeaks supporters, after multiple financial service providers stopped their services for WikiLeaks after the latest, massive disclosure of classified US documents.

The attacks were carried out by using an open source network attack application called Low Orbit Ion Cannon. The attacks were coordinated by using internet forums, Twitter and some C&C servers (Pras et al. 2010; Panda Security 2010; Correll 2010). According to our taxonomy, we classify the motivation as *projecting power*. The functionality of choice was *DDoS* attacks and the participation in this event was *voluntarily*.

4.4 Help-Israel-Win

A *group* of pro-Israel activists, in their campaign against Hamas (*power projection*) set up a website also hosting software for download, to *voluntarily* join a botnet under the control of this group. Based on the information released by this group, they use the botnet to conduct *DDoS* attacks against pro-Palestinian web sites. To which extend they were successful, or if they have launched any attacks at all is still unclear. (Shachtman 2009)

4.5 Conficker

Till now it is publicly not known, who the developers and users of Conficker are. But the analysis of this malware and the speed with which this botnet adapted to counter measures lets us assume, that at least a *group* of persons is behind Conficker. The *lack of any executed functionality* beside file transfer to update the infected clients with last versions of Conficker allows the assumption that Conficker was mainly developed as a proof-of-concept and as such falls under *Education&Research*. Conficker infected its host *involuntary*. (Porras et al. 2009)

4.6 Mariposa

The Mariposa botnet, claimed to be one of the world's largest botnets ever, was developed and used by an international *group* of criminals for *financial gain*. They harvested banking credentials and credit card data (*information theft*) as well as used it for launching *DDoS* attacks. The victims were all infected *involuntarily* (McMillan 2010).

4.7 Belarus censorship

The Belarus state has a longer history of enforcing Internet censorship on its citizens with regards to regime-critical information. Chapter '97, a leading venue for public discussions in Belarus, suffered regularly under state sponsored cyber attacks against their website. In April, 2008 DDoS attack took them down to block state-independent news coverage of protest ongoing in the streets (*manipulation by filtering data*).

While Belarus officials denied official involvement, it is assumed that they were not actively countering the attacks. As such we classify this incident as done by a *state actor*. As the used botnets are unknown, the infection way cannot be decided upon. (Pavlyuchenko 2009)

Table 1: Overview of selected incidents and their classification

Example	User	Motivation	Functionality	Way of infection
Stuxnet	State Actor	Power Projection	Denial of Service	Involuntary
GhostNet	Unknown	Espionage	Information theft	Involuntary
Operation Payback	Group	Power projection	DDoS	Voluntary
Israeli	Group	Power Projection	DDoS	Voluntary
Conficker	Group	Education&Research	none	Involuntary
Mariposa	Group	Financial Gain	Information Theft/ DDoS	Involuntary

5. Conclusions

Easy access to botnets makes them available to all kind of parties, not all of them particularly interested in monetary revenue, but increasingly pursuing political and military aims. With this the common interpretation of monetary motivated cyber crime being the main driver behind the usage of botnet does not sufficiently cover the current situation anymore.

We have presented a usage-centric taxonomy, which provides a structured approach to compare different botnet incidents.

Two distinct applications of the proposed taxonomy were considered; firstly to analyze and categorize past and current botnet incidents. The applicability of the taxonomy has been shown on a selection of recent botnet incidents. The performance of the usage-centric taxonomy in classifying the selected incidents gives hopes that the proposed taxonomy will be helpful in understanding other botnet incidents. This might motivate to structure countermeasures in a similar way and developing an instrument to organize and select responses on different levels.

Another application is to help thinking about novel ways of using botnets. By pre-selecting some attributes, the taxonomy allows for structured and systematic search thru the remaining attributes. By this, the taxonomy might find interesting and novel botnet-related threats and lead to improvements of existing or forthcoming risk assessments and as such helps to improve cyber security on institutional down up to national level.

This taxonomy was designed defining generic taxon, able to be matched even future incidents and is believed to cover most seen so far. Nevertheless the future might show the need to amend the list of taxa, especially the one of *Functionalities applied*.

Disclaimer

The opinions expressed here are those of the authors and should not be considered as the official policy of the Cooperative Cyber Defence Centre of Excellence or NATO.

References

AnonOps, 2010. Welcome to AnonOps Network | Anonymous Operations (AnonOps), HACKERS ON STEROIDS. Available at: <http://www.anonops.ru/> [Accessed February 9, 2011].
 Asosheh, A. & Ramezani, N., 2008. A comprehensive taxonomy of DDoS attacks and defense mechanism applying in a smart classification. *WSEAS Transactions on Communications*, 7(4), pp.281-290.
 Bacher, P. et al., 2005. Know your enemy: Tracking botnets. *The HoneyNet Project*.
 Barford, P. & Yegneswaran, V., 2007. An inside look at botnets. *Malware Detection*.

Christian Czosseck and Karlis Podins

- Champagne, D. & Lee, R., 2006. Scope of DDoS countermeasures: taxonomy of proposed solutions and design goals for real-world deployment. *on Systems and Information Security (SSI)*.
- Correll, S.-P., 2010. 'Tis the Season of DDoS – WikiLeaks Edition | PandaLabs Blog. *Pandalabs*. Available at: <http://pandalabs.pandasecurity.com/tis-the-season-of-ddos-wikileaks-edition/> [Accessed February 9, 2011].
- Deibert, R. et al., 2009. Tracking GhostNet: Investigating a Cyber Espionage Network. *Information Warfare Monitor, Munk Centre, JR02-2009, March, 29*.
- Denning, D.E., 2001. Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy. *Networks and netwars: The future of terror, crime, and militancy*, p.239–288.
- Falliere, N., Murchu, L.O. & Chien, E., 2010. W32. Stuxnet Dossier. *Symantec Security Response*, 3(November), pp.1-64.
- Hansman, S. & Hunt, R., 2005. A taxonomy of network and computer attacks. *Computers & Security*, 24(1), pp.31-43.
- Holz, T. et al., 2008. Measuring and detecting fast-flux service networks. In *Symposium on Network and Distributed System Security*. Citeseer.
- Husted, N. & Myers, S., 2010. Mobile location tracking in metro areas: malnets and others. In *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, p. 85–96.
- Killourhy, K.S., Maxion, R. a & Tan, K.M.C., 2004. *A defense-centric taxonomy based on attack manifestations*, IEEE.
- Klein, G., Leder, F. & Czosseck, C., 2011. On the Arms Race Around Botnets - Setting Up and Taking Down Botnets. In C. Czosseck & K. Podins, eds. *2011 3rd International Conference on Cyber Conflicts*. Tallinn: CCD COE Publications (in press).
- Lemay, A., Fernandez, J.M. & Knight, S., 2010. Pinprick attacks, a lesser included case? In C. Czosseck & K. Podins, eds. *Conference on Cyber Conflict Proceedings*. Tallinn: CCD COE Publications, pp. 183 - 194.
- Lippmann, R.P. et al., 1998. Evaluating intrusion detection systems: the 1998 DARPA off-line intrusion detection evaluation. *Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'98*, pp.12-26.
- McMillan, R., 2010. Spanish police take down massive mariposa botnet. *IDG News*. Available at: http://www.pcworld.com/businesscenter/article/190634/spanish_police_take_down_massive_mariposa_botnet.html [Accessed February 9, 2011].
- Mills, E., 2009. "Golden Cash" network - rent a botnet - ZDNet. *CNET News*. Available at: <http://www.zdnet.com/news/golden-cash-network-rent-a-botnet/312957> [Accessed February 9, 2011].
- Mirkovic, J. & Reiher, P., 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2), p.39.
- Nazario, J., 2009. Politically Motivated Denial of Service Attacks. In C. Czosseck & K. Geers, eds. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press, p. 2010–05.
- Nazario, Jose & Holz, T., 2008. As the net churns: Fast-flux botnet observations. In *Malicious and Unwanted Software, 2008. MALWARE 2008. 3rd International Conference on*. IEEE, p. 24–31.
- Ottis, R., 2008. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. In *Proceedings of the 7th European Conference on Information Warfare*. Academic Conferences Limited, p. 163.
- Panda Security, 2010. The Anonymous cyber-activist group, responsible for the attack on Spain's SGAE and other copyright societies, launches further attacks in defense of Wikileaks founder | Press Panda Security. *Panda Security*. Available at: <http://press.pandasecurity.com/news/the-anonymous-cyber-activist-group-responsible-for-the-attack-on-spain-s-sgae-and-other-copyright-societies-launches-further-attacks-in-defense-of-wikileaks-founder/> [Accessed February 9, 2011].
- Pavlyuchenko, F., 2009. Belarus in the Context of European Cyber Security. In C. Czosseck & K. Geers, eds. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press.
- Porras, P., Saidi, H. & Vinod, Y., 2009. *An Analysis of Conficker*,
- Pras, A. et al., 2010. *Attacks by "Anonymous" WikiLeakers Proponents not Anonymous*,
- Schwartz, M.J., 2010. Pssst...Want To Rent A Botnet? - Darkreading. *Dark Reading*. Available at: <http://www.darkreading.com/security/vulnerabilities/225200525/index.html> [Accessed February 9, 2011].
- Shachtman, N., 2009. Wage cyberwar against hamas, surrender your pc. *Wired*. Available at: <http://www.wired.com/dangerroom/2009/01/israel-dns-hack/> [Accessed February 11, 2011].
- Sophos, 2006. Online Russian blackmail gang jailed for extorting \$4m from gambling websites. *Sophos.com*. Available at: <http://www.sophos.com/pressoffice/news/articles/2006/10/extort-ddos-blackmail.html> [Accessed February 9, 2011].
- Temmingh, R. & Geers, K., 2009a. Virtual Plots, Real Revolution. In C Czosseck & K Geers, eds. *The Virtual Battlefield: Perspectives on Cyber Warfare*. IOS Press, pp. 294-302.
- Temmingh, R. & Geers, Kenneth, 2009b. Virtual Plots, Real Revolution. In Christian Czosseck & Kenneth Geers, eds. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press, pp. 294-302.
- Weaver, N. et al., 2003. A taxonomy of computer worms. In *Proceedings of the 2003 ACM workshop on Rapid Malcode*. ACM, p. 11–18.
- Wood, A. & Stankovic, J., 2004. A taxonomy for denial-of-service attacks in wireless sensor networks. *of Sensor Networks: Compact Wireless and*.
- Wun, A., Cheung, A. & Jacobsen, H.-A., 2007. *A taxonomy for denial of service attacks in content-based publish/subscribe systems*, New York, New York, USA: ACM Press.