DDoS - available weapon of mass disruption

Conference Paper · November 2013

DOI: 10.1109/TELFOR.2013.6716157

1 author:

Vladimir Radunovic
DiploFoundation
4 PUBLICATIONS **4** CITATIONS

DDoS - Available Weapon of Mass Disruption

Vladimir J. Radunovic, *DiploFoundation / Singidunum University*

Abstract — **The increasing militarisation of cyber-space comes in response to fears of critical damage caused by digital weapons like Distributed Denial-of-Service (DDoS). Understanding that the botnets are the key platform behind DDoS, we compared the costs of running a large-scale attack with the approximate downtime loss in a country-scale attack in case of Serbia, showing that DDoS are readily available weapons of possible mass disruption. Taken as a whole, this paper suggests responding to risks by combating cybercrime as the DDoS enabler, rather than by militarisation.**

Key words — **botnet, cyber-attacks, DDoS.**

I. Introduction

The paper explores the availability and the consequences of the Distributed Denial-of-Service (DDoS) type of cyber-attacks with focus on economic aspects. In its first part we outline basic features of the DDoS attacks based on reports and articles related to cases including recent ones, and affirms botnets as almost an exclusive platform for launching the DDoS attacks. In the second part we analyse the availability of DDoS services and botnets based on recent reports about the Russian underground online markets, showing that the investment in establishing a robust platform capable of performing a large-scale attack is in the range of only several thousand Euro. These relatively marginal costs are then confronted in the third part with tremendous economic loss in case of cyber-attacks: based on a known calculation method and related statistical data we showed that the approximate financial loss in a scenario of a country-scale DDoS attack on Serbia goes beyond 10 million Euro per day. In the concluding part, several reflections on the systematic and policy approaches for preventing and responding to the large-scale DDoS attacks are offered, as well as the suggestion about possible further research direction.

II. DDoS and Botnets

Unlike most of the online criminal activities which tend to access computers and data, the Distributed Denial-of-service (DDoS) attacks aim at paralysing the targeted system and thus denying ordinary users to access its resources. In a DDoS attack many computers simultaneously send loads of bogus requests to a targeted system, thereby occupying most of its resources (eg. bandwidth or computing power), thus temporarily disabling legitimate requests to be processed.

Targets of DDoS attacks include web servers of companies, media, public services or other, corporate or government servers especially those providing service to visitors, but also possibly the control servers of national critical infrastructure (like power or water supplies, traffic and communications, industry, etc.) and critical information infrastructure including DNS servers, Internet Exchange Points or data centres. Motives for performing DDoS attacks vary significantly: hactivism, competition and business advantage, support to frauds by distracting from main activities (eg. bank transfer) or disabling the prevention of the fraud, extortion, terrorism and warfare, but also the "active defence" in form of returning the DDoS attack to the identified attacking infrastructure attempting to disable the attackers. However, politically motivated DDoS attacks seem to be the most visible and disruptive [1].

Almost all the DDoS attacks today are based on the use of botnets [2] - networks of hijacked personal computers (bots) that perform remotely commanded tasks without the knowledge of their owners. Size of botnets can be calculated based on various parameters [3], but the order of magnitude is nevertheless scary: for instance, one "army" of 4 million bots from over 100 countries has been dismantled in 2011 [4]. The bots are being controlled remotely by the "Command and Control" (C&C) servers - dedicated or hijacked servers which are under a direct control of the botnet owner ("bot herder") who can, if needed, easily replace them with other compromised computers to avoid detection. Similarly to bots, the C&C servers are also dispersed worldwide - most being recorded in the US, followed by South Korea, China and Russia [5]. Emerging botnet platforms that are based on peer-to-peer technology, in which no C&C servers are needed but the commands are propagated from one to another bot, are much more difficult to track and dismantle.

Disruption power of DDoS botnet is mostly described by the aggregate bandwidth measured at the target end. During the two weeks of the attacks on Estonia in 2007 that disabled most of the e-government and financial services and media, several botnets performed 128 attacks lasting from one to ten hours each, with maximum bandwidth strength at almost 100Mbps [6]. The largest attack recorded by Arbor since 2010 was 100Gbps - a magnitude which "can easily overwhelm a majority of today's Internet access services" [7]. In 2013, however, thanks to many misconfigured DNS servers ("Open resolvers") worldwide, the hosting service CyberBunker performed a DNS-apmlified DDoS on Spamhaus with

Vladimir J. Radunovic, DiploFoundation, Gavrila Principa 44a, 11000 Beograd, Serbia (e-mail: vladar@diplomacy.edu)

bursts of up to 300Gbps [8].

Nevertheless, since most servers will become paralysed under several thousand connections per second, even a relatively modest DDoS botnet can put most of them down. For instance, size of the attack on Estonia regardless of the hard consequences, was not considered significant in scale from the technical point of view [9]. It is the attacking tactics that can improve the effect: attacking the servers that are not public may require finding out the IP addresses of particular critical services; choosing a particular time of attack when the target server is already likely to be very busy; or amplifying the attack through exploiting existing public flaws like the Open resolvers.

The possibly devastating consequences of DDoS attacks on critical infrastructure - and thus on national security - are often used an excuse for the increased militarisation of the cyber-space [10]. The botnets as the bases for launching the DDoS attacks, however, are not part of the military arsenal but are rather "a key part of the infrastructure for cybercrime" [11].

III. AVAILABILITY OF A DDOS BOTNET

"User-friendly" DDoS tools have become readily available on the black online market. A 2012 research by Trend Micro Incorporated [12] explored the services available for sell at the Russian underground market - from renting the DDoS attack as a service, to building own DDoS botnet.

The simplest way is to rent the entire DDoS service, which costs less than 50EUR per day or 100EUR per week; no specific skills are required except for the way to find such offers online. Renting a DDoS botnet, with an option to customise the performances of the attack, costs about 500EUR. These rented services however have some limits. Unlike other types of crimes such as ID theft which may remain unnoticed for long time, the DDoS attacks cause highly visible consequences and can often trigger counter-measures (in form of counter-attacks, complaints to the ISP to cut the service of C&C servers, or investigation by the authorities). The DDoS botnets thus have a higher risk of being dismantled, and the commercial offers are harder to find and are commonly limited in terms of the possible targets (targeting government institutions for instance might not be allowed).

An option more attuned to larger DDoS attacks is to rent an existing botnet and upgrade it with a DDoS capability. A smaller botnet of about 2,000 bots can be rented for about 150EUR; the attacker would then also need to purchase a specific DDoS bot kit, which costs from about 250EUR to about 500EUR, depending on configuration options and ease of use. Renting such a botnet would still likely not allow the attacks (such as on important institutions) that could cause a retort and threat the network existence.

In case of performing a severe attack on important targets including the public institutions or a country-scale attack, a custom-built DDoS botnet might be needed. This would involve several steps:

1. A malware to initially infect large number of computers. A backdoor trojan can be purchased for less than 20EUR, while a malware crypter that would hide it from security software is another 30EUR. Alternatively, a socks bot which may avoid firewalls and can further download malware files (like .exe) from any source would cost about 70EUR.
2. Renting a Pay-per-install service (PPI) to spread the infecting malware around the Internet. PPI inserts the code in various popular online services - fraudulent web sites (porn sites being among most popular), bogus web-ads, user generated content sites and social media tools [5] - tricking the visitors to download it. A "European mix" of targets costs about 60EUR per 1000 downloads of malware, while a global mix costs as few as 10EUR per 1000 downloads. For a DDoS botnet with greater attacking potential, a strong portion of bots from developed countries is needed due to their greater average Internet bandwidths; reaching out to such a mix of 50,000 computers with would yield about 2,000EUR.
3. The initially infected bots now need to receive a DDoS-bot code which would allow for remote control and specific instructions to be issued. A DDoS bot kit, including also the (usually graphic) "command and control" interface costs about 300EUR (with possible regular monthly upgrades).

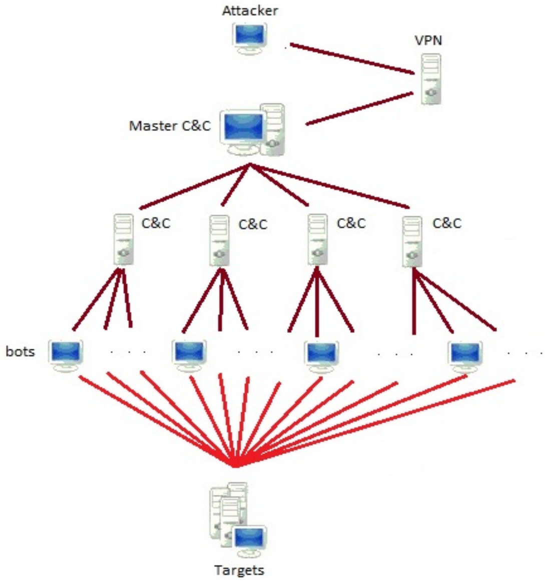

Fig. 1. A scheme of a DDoS Botnet attack

4. Several servers (Fig.1) need to be rented to perform C&C servers (though some can be obtained by hacking the servers on the net). To avoid being taken down due to abuse complains, bulletproof-hosting dedicated servers can be rented for about 150EUR each. In case of planning severe DDoS attacks that might provoke a DDoS retaliation on Master C&C server (once it is uncovered), a special bulletproof hosting service with DDoS protection and 1Gb Internet connection is available for rent for 1,500EUR.
5. As an additional precautious measure, for about 30EUR the attacked may rent a VPN connection

from his own computer to the Master C&C, to avoid suspicion of his own ISP and strengthen his anonymity.

In total, a botnet of about 40,000 DDoS bots can be built for about 6,000EUR. While it is certainly more expensive than renting the service, it has no limits in choosing the targets, can perform very dangerous attacks, and has a number of protective measures. Even if some C&C servers are unmasked and dismantled, an owner of this network can "re-heard" the botnet by downloading new code to bots with different instructions and pointing to new C&C servers. Yet, new bots need to be recruited approximately every six months to replace the disinfected ones [11].

IV. Financial Loss

Dubendorfer, Wagner and Plattner [13] offer an approximated calculation for a financial loss suffered during the Internet outage which can be caused by the DDoS attack. They define the downtime loss as the sum of the productivity loss (i.e. due to limited effectiveness of the employees) and the revenue loss (i.e. due to the inability of an institution or company to fulfil customer requests). In addition to the downtime related loss, they also consider the loss due to disaster recovery, liability due to service level agreements to customers (and possible claims for compensation payments by customers in case of a severe disruption of the service), and the customer loss due to the degraded reputation of the service provider.

The total costs of the Internet outage for the corporations (like main Internet providers, industry or insurance) are predominantly in the liability costs, due to often sky-high claims for penalties defined in the contracts, which exceed the downtime loss and disaster recovery costs by order of magnitude and more. Of the same level of magnitude can be the loss as result of the lost customers - especially with services like e-shops where customers can easily switch to other providers of the service.

It is however interesting to perform the calculation for the "national outage" scenario - similar to the attack on Estonia in 2007 - in which a country-scale DDoS attack is launched by an unknown party lasting for one day (24 hours). According to [13], the value of the total downtime related loss (L_D) is the sum of the productivity and revenue loss during the downtime interval:

$$L_D = \frac{E_{ca}}{d_a} \cdot d_o \cdot E_{no} \cdot E_{po} + \frac{R_a}{ds_a} \cdot ds_o \cdot R_o \cdot S_o \qquad (1)$$

To contribute to findings relevant to developing economies, we will consider the imaginary case of a DDoS attack on Serbia. The following parameters are used:

- E_{ca} (EUR/year) is the annual costs per employee. Since the average gross monthly salary for period January-August 2013 was 59,797 RSD [14], we can take the average annual value as 6,295 EUR[1].
- d_a (hours/year) is the working time per employee per year. Taking the average of 40 hours a week, with 25 days of vacations per year, this yields to 1,880 hours per year.
- d_o (hours) is the working hours overlapping outage time; we take 8 hours which is the average work time per day.
- E_{no} is the number of employees affected by the Internet outage. To approximate this we will firstly take 1,727,048 as the total number of employees in Serbia in 2012 [15]. Observing latest statistics about the Internet usage in Serbia among the population and in companies [16] we will estimate that some 50% of all employees use Internet regularly for their work; with the 24h Internet outage, we can further estimate that only some 60% of these would be affected (mostly in large enterprises and in some of the SME). We will thus take the approximate value of 518,114. It is worth noting that these percentages will only grow with further digitalisation of the Serbian market.
- E_{po} is the productivity degradation during the outage. To estimate this, we will take into consideration several factors: while most of the public administration in Serbia is still not dependant of the Internet ("hard copy" is still largely the default), the work of the corporate sector is increasingly digitalised; most of the communications rely on e-mail exchange, while cloud services such as shared documents and databases are growingly used; not the least, work productivity increasingly depends on the regular search for information online (though productivity may even rise with the inaccessibility of social media tools). Thus, we will take as a very rough approximation that the average productive online time of an employee in Serbia is 20%. Again, it is worth noting that this value will only go up in the years to come.
- R_a (EUR) is the total annual revenue which, in case of Serbia in 2012, equals to 27.75 billion EUR [17].
- d_{sa} (hours) is the service operating hours per year, which we will take is "24/7" yielding to 8,760.
- d_{so} (hours) is a service operation time affected by outage, which equals to the duration of the attack - 24 hours.
- R_o is a part of the revenue affected by the full outage. Since the Internet outage will have a stronger impact on services than on industry and agriculture, and since services present about 60% of the Serbian GDP [18], having in mind the estimated value for E_{po}, we will approximate this value to 10% to be on a safe side. Once again, it is worth noting that this value will only go up in the years to come.
- S_o is a degree of service degradation. Since the scenario refers to a country-wide outage, we will consider it 100%.

The calculated productivity loss based on (1) yields 2,775,768.2EUR, while the revenue loss yields 7,602,739.7 EUR. Thus, the total calculated downtime loss for an imaginary country-scale DDoS attack on Serbia lasting for 24 hours is approximated to 10.4 million EUR. For comparison, the same scenario for Switzerland would

[1] For this and other calculations the exchange rate at the time of writing was used: 1 EUR = 114 RSD

produce a loss of almost 500 million EUR.

Even though the result is only the approximation, possible loss is significant and will only grow with time. Here we should note that the other costs were not included: liability costs mainly stay within Serbia; most of the customers that could possibly be lost are also from Serbia and would not have much alternative choice due to country-wide outage; disaster recovery costs including the efforts to clean the infected computers across the country would be marginal comparing to downtime loss in this scenario.

Additional risk for developing economies is the slow incidence response due to inexistence of Computer Emergency Response Teams (CERT), which may result with the extended duration of DDoS attack (as was the case with Estonia in 2007). In such case, the downtime loss grows steeply, since the values of affected employees (E_{no}), productivity degradation (E_{po}) and part of the revenue (R_o) will be greater than those for 24h attack

V. Conclusion

DDoS tools and services are readily available on the market for anyone with almost basic understanding of the potentials, and can be rented or built with symbolic investments in range of several hundred to several thousand Euro, depending on complexity, robustness and strength. The financial consequences of a mass disruption such tools can cause to corporate sector or government services are several orders of magnitude higher, with a calculated loss in case of a 24-hours long country-scale Internet downtime in Serbia over 10 million Euro. Consequences can be more devastating in case of the attack on the servers controlling the national critical infrastructure.

To reduce risks, states should have policies in place related to prevention of and incident response to DDoS attacks. In terms of prevention, a focus on proper “computer hygiene” (regular patching and updates of software, firewalls and antiviruses) and responsible online behaviour - among users and especially within companies and institutions - can prevent the spread of malware infections and the emergence of bots. Proper configuration of key network equipment, including disabling the Open resolvers, can reduce the risks as well. Additionally, following also the cyber-security strategy of the European Union which puts the combat against botnets and malware as one of the priorities [19], a cross-border cooperation in fighting the malware and botnets (both through technical and the legal means) should be strengthened.

In terms of incident responses, the existence of CERT on national, government and corporate levels has become a must. Unfortunately, many countries including Serbia still don’t have the CERT which increases the risks of extended duration attacks with more severe consequences, as well as of “active defence” DDoS responses targeting the compromised computers acting as C&C servers (some of which may in fact be important controllers of the critical infrastructure) due to inexistence of a country’s single point of contact for incidents. While CERT should also help identifying the existing bots and C&C servers, cleaning them up by users and experts may be costly and may not effectively dismantle the botnet since they can be rebuilt easily with modest payments to PPI services. Further research work is thus needed with regards to the efficient combat against the botnets as the main platform for running the dangerous DDoS attacks.

Literature

[1] J. Nazario, “Politically Motivated Denial of Service Attacks”, in *Cryptology and Information Security Series, Volume 3: The Virtual Battlefield: Perspectives on Cyber Warfare*, C. Czosseck K. Geers, Ed. 2009, pp. 163 - 181.

[2] (Online source) L. Greenemeier. (2007, 05, 18). *Bots Hammer Estonia In Cyber Vendetta* [online]. Information Week. Available: http://www.informationweek.com/bots-hammer-estonia-in-cyber-vendetta/199602023

[3] M. Abu Rajab, J. Zarfoss, F. Monrose, A. Terzis, “My Botnet is Bigger than Yours (Maybe, Better than Yours) : why size estimates remain challenging,” in *Proc. 1st Conf. on Hot Topics in Understanding Botnets*, Berkeley, 2007, pp.5

[4] (Online source) V. Radunovic. (2011, 11, 18). *‘Operation Ghost Click’: Cyberzombies in the real world* [online]. Internet Governance Blogs, DiploFoundation. Available: http://www.diplomacy.edu/blog/%E2%80%98operation-ghost-click%E2%80%99-cyberzombies-real-world

[5] (Report) *The Advanced Cyber Attack Landscape report*. FireEye Inc, 2013.

[6] (Report) B. Toth, “Estonia under cyber attack”, Hun-CERT, 2007. Available: http://www.cert.hu/sites/default/files/Estonia_attack2.pdf

[7] (White Paper) *Anatomy of a Botnet*. Arbor Networks, Inc, 2012.

[8] (Online source) V. Radunovic. (2013, 04, 02). *Waging a (private) cyberwar* [online]. Internet Governance Blogs, DiploFoundation. Available: http://www.diplomacy.edu/blog/waging-private-cyberwar

[9] (Online source) S. Waterman. (2007, 06, 11). *Analysis: Who cyber smacked Estonia?* [online]. United Press International. Available: http://www.upi.com/Business_News/Security-Industry/2007/06/11/Analysis-Who-cyber-smacked-Estonia/UPI-26831181580439/

[10] V. Radunovic, “Pacifizam u kiber-prostoru: zašto je za kiber-bezbednost važnija saradnja među sektorima i akterima nego njegova militarizacija,” in *Proc. Conf. Informaciona bezbednost 2013*, Belgrade, 2013.

[11] R. Anderson, C. Barton, R. Boehme, R. Clayton, M.J.G. van Eeten, M. Levi, T. Moore, S. Savage, “Measuring the Cost of Cybercrime,” in *Proc. of the Workshop on the Economics of Information Security (WEIS)*, Berlin, 2012.

[12] (Research Paper) M. Goncharov, “Russian Underground 101”, Trend Micro Incorporated, 2012. Available: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

[13] T. Dubendorfer, A. Wagner, B. Plattner, “An Economic Damage Model for Large-Scale Internet Attacks”, in Proc. 13th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2004, pp. 223 - 228.

[14] (Statistics) “Zarade po zaposlenom u Republici Srbiji po oblastima delatnosti, avgust 2013”, *Saopstenje broj 263*, Republički zavod za statistiku, Republika Srbija, 2013. Available: http://webrzs.stat.gov.rs/WebSite/repository/documents/00/01/14/27/zp11092013.pdf

[15] (Statistics) “Broj zaposlenih - ukupno, godisnji prosek, 2012”, Republicki zavod za statistiku, 2013.

[16] (Report) “Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji, 2013”, Republički zavod za statistiku, Republika Srbija, 2013.

[17] (Online resource) World Bank, 2012. Available: http://search.worldbank.org/data?qterm=GDP+serbia&language=EN&format=

[18] (Online resource) “The World Factbook”, Central Intelligence Agency, 2013. Available: https://www.cia.gov/library/publications/the-world-factbook/geos/ri.html

[19] (Policy document) “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace”, (2013, 02, 07), *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, European Commission, Brussels.