Chapter 7
Modeling the Economic Incentives of DDoS Attacks: Femtocell Case Study *

Vicente Segura, Javier Lahuerta

Abstract Many of the Internet security incidents are caused by agents which act moved by economic incentives. When that is the case, it is possible to model attacker's incentives by applying economics principles and, if we can collect appropriate data, we can use the model to have a better understanding of the risk imposed by these threats. This paper presents a simple model that represents the economic incentives for launching DDoS attacks against a specific telecommunications service. In addition, some data has been collected in order to quantify some of the variables of the model. Finally, some simulations have been performed to have a better knowledge of the risk of suffering this kind of attacks and propose solutions to mitigate it.

7.1 Introduction

Risk analysis and management methodologies provide procedures and techniques for identifying and estimating security risks, identifying possible countermeasures and estimating how they reduce risks. Since now, these methodologies have proved to be useful for the systematic identification of risks. However, their usefulness for risks quantification is a very polemic topic. As Bruce Schneier says [12], one of the main reasons can be the scarcity of available data to estimate the variables in which the risk calculation models are based.

Most of the time, collecting suitable data in order to make reliable risk estimations is quite difficult or has unacceptable costs. Sometimes, risk analysts face these difficulties using qualitative scales for risk estimation. Although it does not provide

Vicente Segura, Javier Lahuerta
Department of Network and Services Security, Telefonica I+D, e-mail: vsg@tid.es

* This material is based upon work supported by the SEGUR@ Project, funded by the Centre for the Development of Industrial Technology (CDTI) of the Spanish Ministry of Science and Innovation.

T. Moore et al. (eds.), *Economics of Information Security and Privacy,*
DOI 10.1007/978-1-4419-6967-5_7, © Springer Science+Business Media, LLC 2010

either a clear knowledge of risks magnitudes or a return-of-investment analysis of countermeasures, it enables the prioritization of risks. Anyway, when using qualitative or quantitative measures, we need procedures or techniques to estimate risk factors in a systematic and objective way. Similar results should be reached by different analysts when analyzing the same scenario.

This paper describes the details and results of a work in which we have modeled the economic incentives behind DDoS attacks against a specific telecommunications service. We think this is an example of systematic procedure that can be used to estimate risk factors when there is an economic motivation. It seems that it is what happens in an increasing percentage of cases due to the rising specialization of cybercrime [13]. In this situation, attacker's behavior is rational and even predictable. Therefore, it is possible to model the conditions that influence the attacker's behavior and, if we can collect data about our particular scenario we can estimate some risk factors, such as the probability of being impacted by some threats.

This paper focuses on a specific service which some European mobile operators will start to provide soon and which is already available in USA and in some Asian countries [4]. This service extends and improves the mobile coverage inside the home of its customers by means of a device called femtocell that links to the operator core network through a broadband line, typically an ADSL line. Femtocells are connected to the operator core network through a device called security gateway. The service architecture has a radical difference with respect to traditional architecture of mobile operator networks. They have been typically quite isolated from the Internet, but now the security gateway is the linking point between femtocells and the operator core network and it must be accessible from external networks that, in some of the proposed deployments, include the Internet.

The rest of the paper is organized as follows. Section 2 focuses on describing some of the previous works developed by different researchers that have some relation with this paper. Section 3 develops the economic model. Section 4 applies the model to the telecommunications service and it is composed of three subsections: data collection, analysis of collected data and use of the model to assess the economic incentives under different assumptions. Finally, section 5 concludes this paper.

7.2 Background and Related Work

Most of the research works about DDoS attacks and the main instrument to carry them out, botnets, have mainly considered technical aspects and have tried to understand how the botnets work, its topologies and their use. In the last years, some of the works have started to complement this technical approach with an economic analysis whose main objective consists in modeling the economic incentives of the attackers and in finding strategies to mitigate risks.

This work belongs to this second group of works. This section describes some of the research works developed up to now and compares them with the one described in this paper.

The study by Liao et al. has some similarities to ours [10]. They propose an economic model for representing the incentives of both actors: the attacker who rents a botnet for launching a DDoS attack and the botnet master who owns that botnet. The attacks will only happen if both obtain benefits. Their goal is to model how the introduction of virtual bots affects the benefits. However, they do not apply the model to any specific scenario using real data. Our work focuses in applying the model to a specific scenario and we have collected some data, such as the cost of hiring a service for launching DDoS attacks.

In another study [5], Franklin and Perrig analyze data collected from the underground markets and propose two possible techniques that hinder transactions. Both try to damage sellers' image so that it increases uncertainty and distrust among possible buyers. Our work focuses in a specific threat, DDoS attacks, and in the prices for launching them, but both works uses data collected from underground markets in order to apply an economic model and propose solutions to mitigate risks.

Another similar work developed by Ford and Gordon [6] focuses on analyzing the revenue generated by malicious code. They do not focus on a single threat but consider the whole set of malicious activities that can provide revenue to botnet controllers such as adware, confidential data sales or renting botnets for launching DDoS attacks. On the other hand, it is a theoretical model and they do not try to apply it to a real scenario.

Last but not least, Friess and Aycock analyze the business case of using botnets for collecting and selling personal information [7]. Although we analyze the use of botnets for other malicious activities, there are some similarities between both works because they develop the business case in order to identify possible defense strategies. In our work, we also use our model to identify how the different defense strategies reduce attack profits.

7.3 The Model

In order to collect data from Internet underground markets we have been analyzing advertisements published by cybercriminals and we have been talking to them through instant messaging clients. The main conclusion we can extract from this activity is that most of them are specialized in concrete activities. Of course, it is possible that someone builds its own botnets in order to launch DDoS attacks and extort victims on her own although it seems that it is not very common. The simplest and less risky way for someone who wants to extort a victim is to hire this service. There are many cybercriminals that are specialized on launching this kind of attacks. They just need an IP and some dollars.

Therefore, our model assumes that there is a high specialization of activities in the underground market and that if someone wants to extort an organization, just needs to hire this service to a botnet master.

The attacker hopes to obtain some revenue by extorting the victim. As a result, the expression for modeling the profit will be as follows:

$$Profit = E - C > 0; \tag{7.1}$$

where E represents the attacker's revenue and C the cost of hiring the DoS service.

This is a general expression for any affected service as we are not considering the particular features of the service yet. Then, the next step consists in analyzing our particular service and identifying the variables that influence in some way the components of the equation 7.1.

The figure 11.1 shows the general scenario of the telecommunication service analyzed in this paper. Residential femtocells are connected to the mobile operator core network through a device called security gateway. Mobile operators' infrastructures have more than a security gateway and each one will have a different IP address. Thus, the attacker will need to launch different DDoS attacks for each of them. We assume that the attackers will arrange the attacks independently for each target gateway. Therefore our model represents the incentives for launching a DDoS attack against a specific security gateway.

We assume that the security gateway links with a total set of "n" femtocells through IPSEC tunnels that encrypt the data that travels between the peers. In addition, the security gateway is able to process up to "r" Gbps of data.

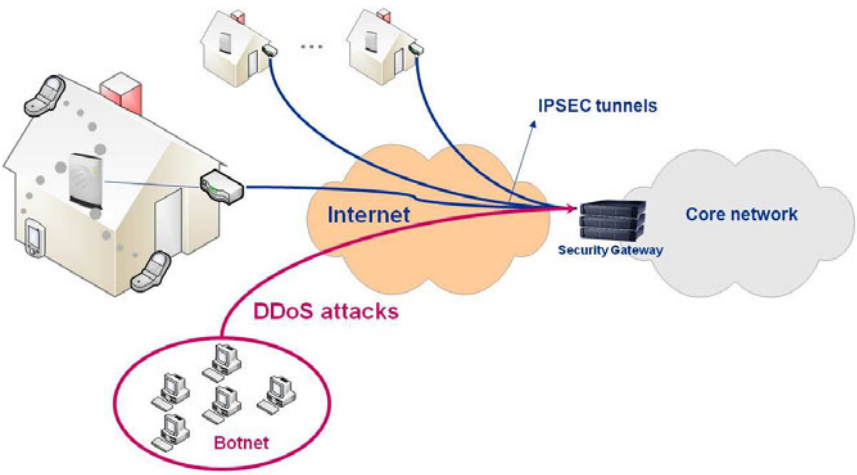

Fig. 7.1 Scenario of the telecommunication service: extended and improved coverage of mobile networks in the residential environment with femtocells.

It would be possible to leave homes without service by launching a DDoS attack that depletes the data processing resources of the security gateway, i. e. an attack of "r" Gbps or higher. The typical DDoS attack against a gateway that sets IPSEC tunnels with several clients is an IKE_SA_INIT flood. Therefore, we assume that any attacker which wants to extort the network operator will have to launch an IKE_SA_INIT flood attack of this bandwidth or higher.

Regarding extortion revenue, we must say that its modeling is much more difficult due to the scarcity of data about this kind of malicious activity. It seems reasonable to assume that the amount asked by attackers should depend on the annual revenue of the mobile operator. It is at least what has happened with online gambling site extortions, one of the more affected businesses by DDoS attacks. The amount asked to them have ranged from 10 000$ to 40 000$ depending on their annual revenues [8, 9]. But asking for an amount of dollars does not mean that the victims pay it. In fact, we hope that mobile operators do not give in to blackmail, as experts and police authorities have recommended, because the less victims giving in to blackmail, the less economic incentives for attackers. However, many news warning about the high percentage of organization that ended up giving in to blackmail have been published [9, 11]. Therefore, at least until mobile operators demonstrate clearly to cybercriminals that they are not going to follow the same way, we think that it is possible that attackers hope that could happen something similar as with online gambling sites. Based on that all, we propose to model the extortion with the following equation:

$$E = \alpha \cdot f(R) \tag{7.2}$$

where α means the percentage of victims that the attacker hopes that will give in to blackmail and $f(R)$ is a function of the victim's annual revenue.

The annual revenue depends on the number of femtocells per security gateway and the average revenue per femtocell. Thus, we can rewrite the equation as follows:

$$E = \alpha \cdot f(nAR) \tag{7.3}$$

where n is the number of femtocells per security gateway and AR is the average annual revenue per femtocell.

We have not been able to infer the function that relates the extortion with the revenue because we have not found concrete data about online gambling site's revenue and the amount of dollars that they have been asked for. However, we know by the references mentioned before that the amount of the extortion was between 10 000$ and 40 000$ during 2004. We have compared these amounts with the annual revenue of some of the online gambling sites [1, 3, 14] and we have seen that they are approximately 1,000 times smaller. Thus, we will use the following equation for simulation:

$$E = \alpha \cdot k \cdot n \cdot AR \tag{7.4}$$

where k is 0.001.

7.4 Application of the Model

We have arranged this section in three subsections. The first one explains how we have collected the data for applying the model. The second one shows the results of a regression analysis that allowed us to estimate the cost of renting a botnet as a function of the bandwidth and the duration of the DDoS attack. The last one uses the results of former subsections to assess attacker's incentives.

7.4.1 Data Collection

In this section we describe how we collected data for estimating both the revenue of attackers and the cost of hiring the DDoS attack service.

7.4.1.1 Extortion Revenue

In the previous section we stated that the attacker's revenue depends on these factors:

- α, the percentage of victims that will give in to blackmail,
- k, a constant whose value is 0.001,
- $R = n \cdot AR$, the annual revenue.

Regarding the first factor, we have not found data or surveys to assess its value. The lack of legislation that forces victims to communicate if they have given in to blackmail and the fear to bad reputation are two reasons that can explain this absence of data.

We consider that there are 20,000 femtocells per security gateway, as it is the number of tunnels that can provide some of the typical devices used in these architectures, such as the Alcatel-Lucent VPN Firewall Brick 1200.

Finally, a business case study from Analysis Research [2] provides an estimate of the average revenue per femtocell. In this study they consider 4 different customer profiles based on the number of handsets per home and the indoor coverage quality. We take the optimistic estimation because it is the worst case for us as it gives the largest incentives for launching the attack. It considers that the service will provide an additional monthly revenue of 28$ per femtocell. Therefore, the annual revenue per security gateway is:

$$R = n \cdot AR = 20,000 \cdot 28 \cdot 12 = 6,720,000\$/year \tag{7.5}$$

And we have the following equation for the extortion revenue:

$$R = \alpha \cdot k \cdot n \cdot AR = \alpha \cdot 6720\$ \tag{7.6}$$

7.4.1.2 Cost of Hiring the DDoS Attack Service

There are plenty of forums in the Internet where one can access to hire this kind of services. This has been our main source of information in this work. We have looked for advertisements where cybercriminals offer this service and we have talked to them through instant messaging applications, mainly the ICQ client, in order to know how the price of the service changes with its particular features. It seems that the cost depends mainly on the bandwidth of the attack and its duration. The figure 11.2 shows the translation of one of the advertisement in a Russian forum.

Part of one of the conversations with a service provider in which we asked for the price of a service with a specific duration and bandwidth can be seen in figure 11.3.

The set of collected prices is shown in the table 7.1.

7.4.2 Regression Analysis for the Cost Function

We have performed a regression analysis using the data showed in the previous table in order to determine the cost of the service as a function of its bandwidth and its duration. The function type that adapts better is a Cobb-Douglas one:

$$C = L \cdot A^{\gamma} \cdot t^{\beta} \tag{7.7}$$

where:

- C, is the cost of hiring the service,

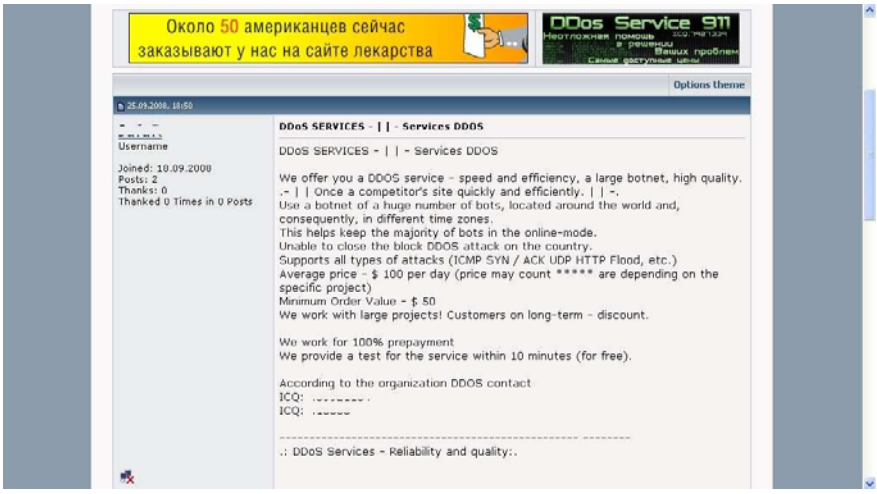

Fig. 7.2 A DDoS Service advertisement in a Russian forum.

Table 7.1 Cost of the service for different bandwidth and duration.

Price ($)	Duration (h)	Bandwidth (Mbps)
20	2	45
30	6	45
50	12	45
70	24	45
75	24	100
250	24	1000
100	24	1000
600	168	1000
900	24	4750
1000	24	4750
5500	168	4750
6000	168	4750
400	5	5000

- L, is a constant,
- A, is the bandwidth depleted by the attack in Mbps,
- t, is the duration of the attack in hours,
- γ, is the cost elasticity of the bandwidth and,
- β, is the cost elasticity of the duration.

In order to apply a linear regression, first we need to transform the equation:

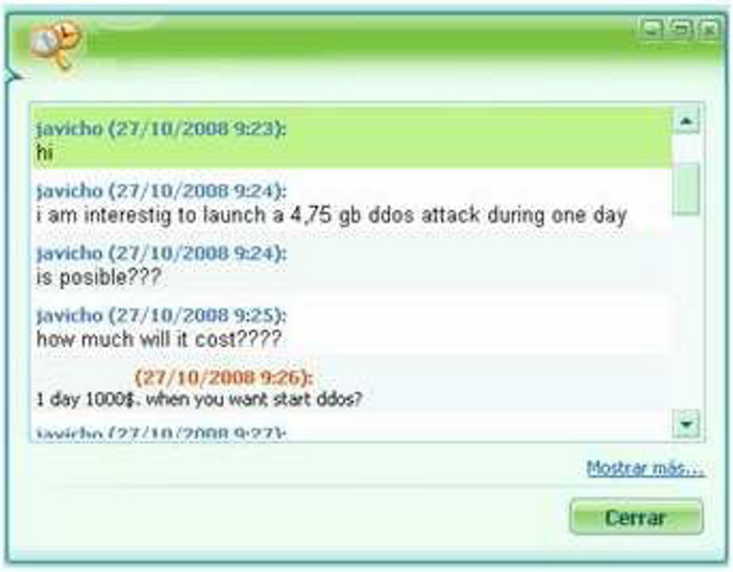

Fig. 7.3 An example of conversation with a DDoS service provider.

Table 7.2 Results of the regression analysis ($R^2 = 0.915$; adjusted $R^2 = 0.898$).

Variable	Value	Standard error	t-statistic	P-value
K	-0.036765	0.568531	-0.064668	0.9497
γ	0.586899	0.095469	6.147523	0.0001
β	0.590331	0.146111	4.04028	0.0024

$$ln(C) = K + \gamma \cdot \ln(A) + \beta \cdot \ln(t) \tag{7.8}$$

We have obtained the following results:
Therefore, the resulting function is as follows:

$$ln(C) = -0.0367 + 0.5869 \cdot \ln(A) + 0.5903 \cdot \ln(t) \tag{7.9}$$

Once transformed to its original form:

$$C = 0.9640 \cdot A^{0.5869} \cdot t^{0.5903} \tag{7.10}$$

Both the absolute value of γ and β t-statistics are greater than 2. Thus, we can assure that there is a strong relation between the two independent variables and the dependent variable. In addition, both R-squared and adjusted R-squared are greater than 0.8 which means that the function represents the relation between the cost and the independent variables with acceptable accuracy.

7.4.3 Use of the Model to Estimate the Economic Incentives for Launching DDoS Attacks

If we substitute in equation 7.1 the expressions for the revenue and costs of the attacker, we obtain the following expression for the profit:

$$Profit = E - C = \alpha \cdot 6720 - 0.9640 \cdot A^{0.5869} \cdot t^{0.5903} \tag{7.11}$$

It seems reasonable to think that the greater the profits the greater the probability of DDoS attacks. On the other hand, potential attackers lose economic incentives when the profit is zero or lower.

The remainder of this section contains three simulations that we have performed using the equation 7.11. For each one we have made some assumptions that are represented with a constant value for some of the variables (α, A and t). Then, we can analyze what values must have the rest of the variables in order to nullify the profit which can be used to identify strategies to protect against the attacks.

7.4.3.1 Simulation 1

In our scenario, the security gateway is able to resist DDoS attacks of up to 4750 Mbps. In addition, we assume that the attacker needs to hire a 24 hours service in order to force the victim to pay. Then, the profit function is as follows:

$$Profit = E - C = \alpha \cdot 6720 - 0.9640 \cdot 4750^{0.5869} \cdot 24^{0.5903} \tag{7.12}$$

To nullify the incentives, the following condition must be met:

$$\alpha \leq \frac{0.9640 \cdot 4750^{0.5869} \cdot 24^{0.5903}}{6720} = 0.1347 \tag{7.13}$$

That means that if the percentage of victims that does not give in to blackmail is 13.47

7.4.3.2 Simulation 2

Let's assume now that a 20% of victims pay and that the duration of hired attacks must be 24 hours. We can calculate the resistance that our infrastructure must have in order to nullify economic incentives:

$$Profit = 1344 - 0.9640 \cdot A^{0.5869} \cdot 24^{0.5903} \tag{7.14}$$

In figure 11.4 we can see how the profit decreases as bandwidth increases. It also can be seen that there is a bandwidth that nullifies economic incentives: 9320 Mbps.

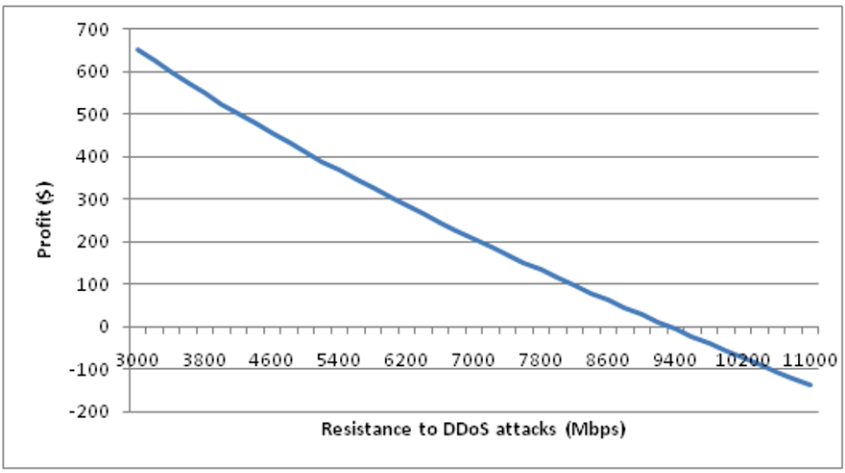

Fig. 7.4 Attacker's profit as a function of the resistance to DDoS attacks.

With a resistance of 4750 Mbps as the one we had initially, launching DDoS attacks would be profitable for an attacker. At that point, the victim has at least two possible strategies in order to reduce the probability of being the victim of these attacks:

- to deploy a security gateway that is resistant to DDoS attacks of 9320 Mbps or higher or
- to design a network architecture that increases the cost of the attacks. Instead of allowing every Internet IP addresses to reach the security gateway, only IP addresses from customers of this service should be allowed. Thus, successful attacks should be launched by bots installed on customer's PCs. It would set a special requirement to botnets that would increase significantly the cost of hiring successful DDoS attacks.

7.4.3.3 Simulation 3

Let's assume again that the duration of attacks must be 24 hours. Then, we can derive the relation between the bandwidth and the percentage of victims that pay that nullify the incentives:

$$Profit = \alpha \cdot 6720 - 0.9640 \cdot A^{0.5869} \cdot 24^{0.5903} = 0 \tag{7.15}$$

$$A = \left(\frac{6720}{0.9640 \cdot 24^{0.5903}}\right)^{1.7039} \cdot \alpha^{1.7039} \tag{7.16}$$

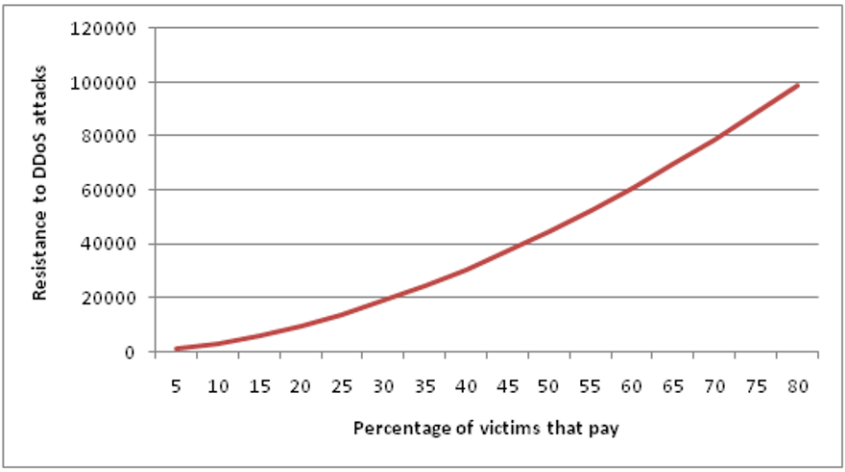

Fig. 7.5 Resistance to DDoS attack that is needed in order to nullify incentives.

The relation between A and α has been represented in figure 11.5. It shows that the resistance increases quickly with the percentage of victims giving in to blackmail.

7.5 Conclusion

The economic motive seems to be one of the main pushing forces of the Internet security incidents. When it happens, attackers' behavior is rational and, even, predictable. Under some assumptions, it is possible to model the conditions that will influence the attacker's behavior and, if we are able to collect data for our model, we can estimate the probability of the attacks.

This paper has focused on applying a simple economic model to a real scenario based on a telecommunication service that many mobile operators will start providing in the short term and that some of them are already providing. This model represents the incentives of a potential attacker for launching DDoS attacks. To apply the model we have collected data from two sources. On one hand, we have searched Internet underground markets to collect prices of hiring DDoS attack services. On the other hand, we have used existing information about past extortions against online gambling sites to estimate the amounts of money that attackers could demand in our service.

The analysis performed in this work is a first attempt to estimate the incentives for launching DDoS attacks based on objective data. We know that the proposed model can be not complex enough to cover some possible situations such as the victims agreeing not to pay up any more, but we preferred to keep the model simple enough so as to apply it to real scenarios using available data. We think the model can be further refined and the technique followed in this work can be used to assess the factors that have influence on risks when there is an economic motivation behind the incidents. In our opinion, that could complement current risk analysis methodologies.

Applying this technique can be hard because of the scarcity of the necessary data. In our case, we have had to contact cybercriminals willing to provide the service, explain them the features of the attack and try to obtain the price of the service. This has not been easy because they tended to mistrust us, especially after using the same ICQ identifier to ask prices to different people. We think that they are well organized and warn each other when there is someone behaving suspiciously.

But understanding better how they are organized and collecting data about the underground markets in an easier and more frequent way would allow us to know and assess more reliably the risks of cybercrime for any service which depends on the Internet. There is plenty of work to do in this field. We hope that our work has contributed somehow to it.

References

1. BETFAIR: Annual Report (2004). http://corporate.betfair.com/key-data/5-year-financial-summary.html
2. Brydon A., Heath M.: Femtocells in the consumer market: business case and marketing plan. Analysis Research (2007)
3. BWIN: Annual Report (2004).
4. Femtoforum: Femtoforum newsletter February (2009). http://www.femtoforum.org/newsletters/newsletter04/index.html
5. Franklin, J., Paxson, V., Perrig, A., Savage, S.: An inquiry into the nature and causes of the wealth of Internet miscreants. In: Proceedings of the ACM Conference on Computer and Communications Security (CCS), pp. 375–388. ACM Press, New York (2007)
6. Ford, R., Gordon, S.: Cent, five cent, ten cent, dollar: Hitting spyware where it teally hurt$. In: Proceedings of the New Security Paradigms Workshop (NSPW), pp. 3–10. ACM Press, New York (2006)
7. Friess N., Aycock J.: Black market botnets. In: MIT Spam Conference. Cambridge, MA (2008)
8. IDG News Service: Super Bowl fuels gambling sites' extortion fears. IT World, 28 January (2004). http://www.itworld.com/040128gamblingsites
9. Ilett, D.: Expert: Online extortion growing more common. CNET, 8 October (2004). http://news.cnet.com/Expert-Online-extortion-growing-more-common/2100-7349_3-5403162.html
10. Li, Z., Liao, Q., Striegel, A.: Botnet economics: Uncertainty matters. In: M.E. Johnson (ed.) Managing Information Risk and the Economics of Security, pp. 245–267. Springer, New York (2008)
11. Pappalardo, D., Messmer, E.: Extortion via DDoS on the rise. Computerworld, 15 May (2005). http://www.computerworld.com/networkingtopics/networking/story/0,10801,101761,00.html
12. Schneier, B.: Does risk management make any sense? (2008). http://www.schneier.com/blog/archives/2008/10/does_risk_manag.html
13. Symantec: Symantec Internet Security Threat Report XIII (2008).
14. UNIBET: Annual Report (2004). http://www.unibetgroupplc.com/corporate/templates/KeyFigureList.aspx?id=113