Informal Economics of Information Threats

Serghei Ohrimenco[1], Grigori Borta[2]
[1]Laboratory of Information Security, Academy of Economic Studies of Moldova
osa@ase.md
[2]Laboratory of Information Security, Academy of Economic Studies of Moldova
grigori.borta@gmail.com

Abstract. This paper attempts to define shadow information economics as a domain of knowledge that aims at designing and implementing information threats (e.g. malware, DDoS attacks, etc.). This paper also analyzes and explores economical basis of shadow information economics functioning. An economical model of information threats is proposed.

Keywords: information security, information economics, shadow information economics.

1. Introduction

The phenomenon of shadow information economics is, according to our opinion, not sufficiently studied, even though it remains an important problem in the computer era, where cybercrime becomes a problem, that every user has come across. This paper tries to draw researchers' attention to the problem of shadow information economics.

2. Definition

We define shadow information economics as all the individual and collective unlawful activity, related to design, production, distribution, support, and use of components of information and communication technologies that is hidden from society. In other words, shadow information economics is all the criminal information products, services and processes based on IT or using IT. The main economical elements of this domain are unlawful economical relationships, illegal business, which is related to production, distribution and use of prohibited goods and services, sphere of illegal employment. It is important to note the fact that this kind of economics merges unlawful goods and services production, prohibited by national legislations, unlawful sale and purchase of goods and services, and consume of aforementioned unlawful goods and services. Therefore, we can conclude that the main reason of shadow economics existence is a set of conditions that makes it profitable to conduct unlawful activity in the domain of information technologies.

3. The Threats

A threat in information security is possible danger of a vulnerability being used to overcome system defense and cause damage. ISO 27005 defines a threat as follows: "a potential cause of an incident, that may result in harm of systems and organization". NIST defines a threat as: "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability". Therefore, we can derive the following categories of threats:

- unauthorized access
- destruction
- disclosure

- modification of information
- denial of service

A research by Spy Ops, Technolytics, and Intelomics defines the following cyber threats:

- Logic Bomb
- Computer Virus
- Rabbit
- Bacterium
- Spoofing
- Sequential Scanning
- Dictionary Scanning
- Digital Snooping
- Spamming
- Tunneling
- Scavenging
- Counterfeit Equipment
- Counterfeit Software
- Software Malfunction
- Botnets
- Trap / Back Door
- TEDs / EPFCs / EMP
- Insider Threat
- Trojan Horse

The research defines a rating and a color code for each of the threats.

Threats may be classified by their type (physical damage, natural events, loss of essential services, information compromise, technical failures, and function compromise) and origin (deliberate, accidental, and environmental).

Another research, by Digital Forensics Association, covering 28 countries and 3700 incidents, shows that the main vectors of information breaches are hacks, removable storage, web, fraud (social engineering), and lost laptops.

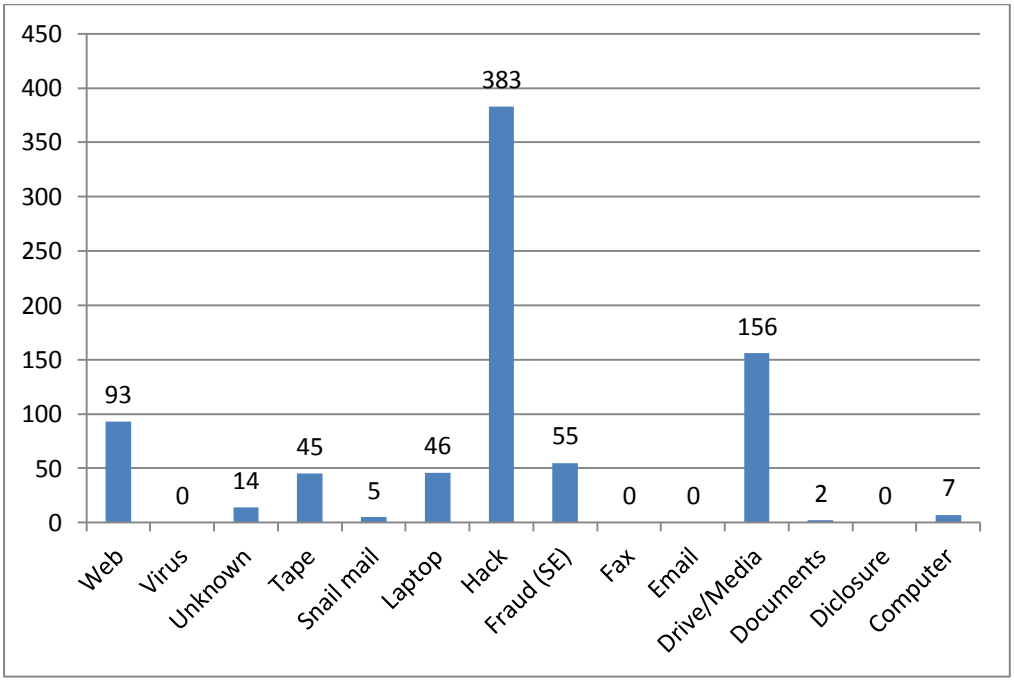

Figure 1. Information disclosure according to Digital Forensics Association

A report by Symantec confirms that in 2012 the most usual cause of data breaches were hackers, being the cause in 40% cases, with accidental disclosure and loss of computers or drives being close second, both being the cause in 23% cases.

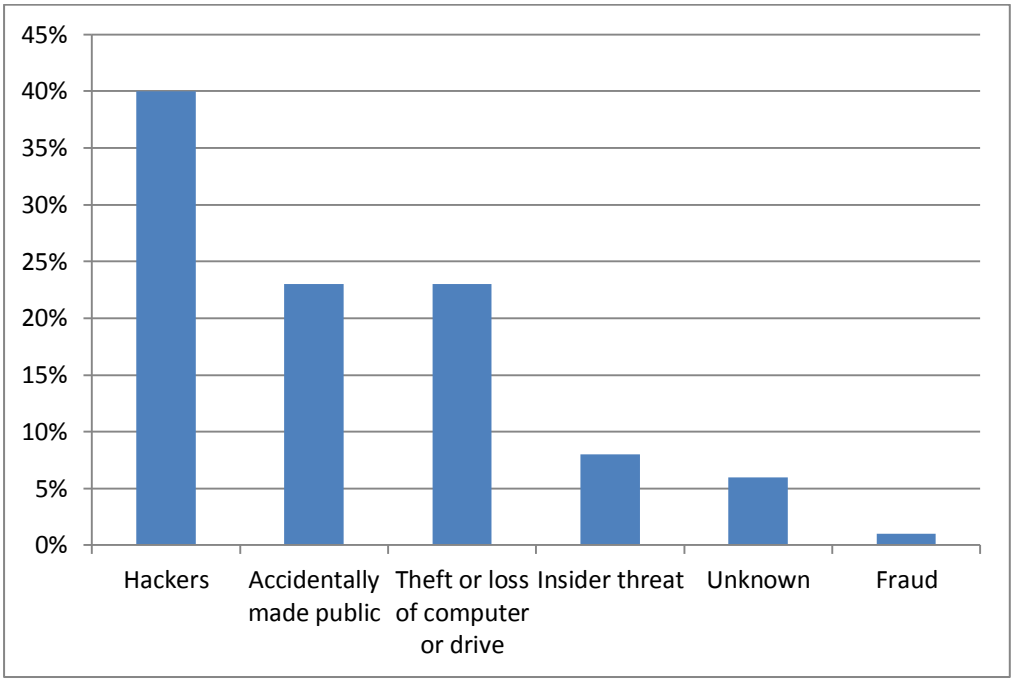

Figure 2. Data breach vectors in 2012 according to Symantec

The same report suggests that the number of targeted attacks has grown by 42% compared to the previous year. This type of attacks more often targets smaller companies than before. According to Symantec, most of the attacks target manufacturing (24%), with Finance, Insurance & Real Estate and Services – Non-Traditional being on the second and third places, having 19 and 17 percent respectively.

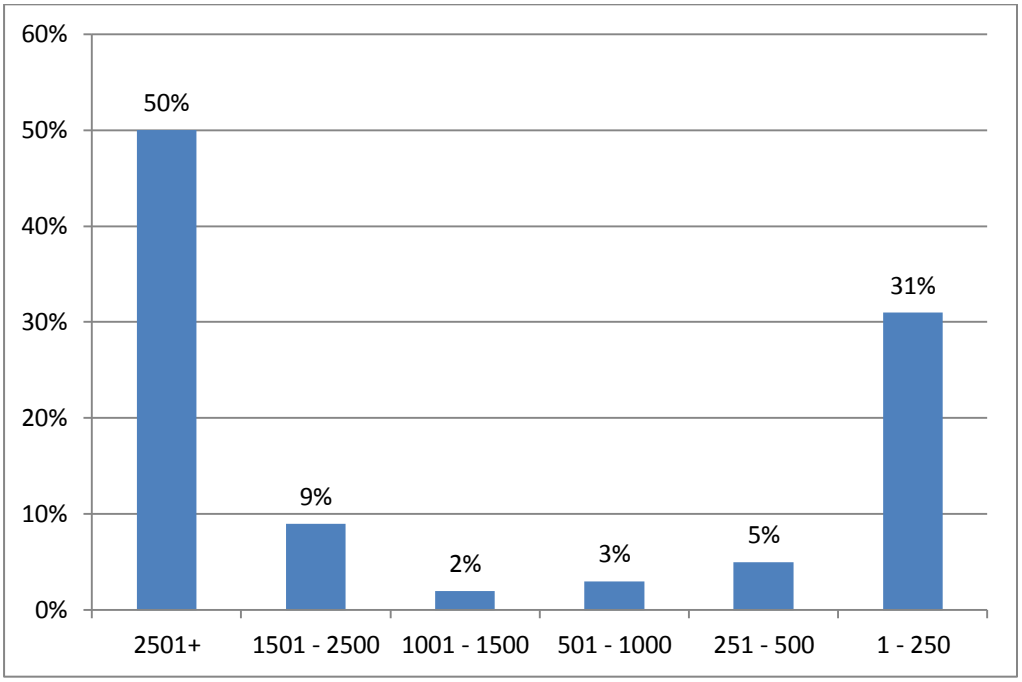

Figure 3. Number of attacks, depending on the enterprise employees number accordin to Symantec

4. Structure

In the table 1 we provide a comparison between classical legal economics, classical shadow economics and shadow economics in the information technologies.

Table 1. Economics comparison

	Legal Economics	**Shadow Economics**	**Shadow Information Economics**
Goal	Satisfying consumer needs, maximizing profit using legal means	Satisfying destructive needs, maximizing illegal profit	Satisfying destructive needs, maximizing illegal profit
Relationship basis	Property relationship	Illegal use of property	Illegal use of property
Forms of property	• Private • State • Combined	• Private • State	• Private • State

Production, distribution, exchange and consumption	Related to forms of property	Illegal goods and services	Illegal goods and services
Methods and forms of activity	• Private • State • Combined	• Private • State	• Private • State
Management models	• Liberal • Neo-liberal • Keynesian • Japanese	• Arborescent	• Arborescent
Competition	Adjustable, intra-sector, inter-branch, combined (fair business conditions), imperfect competition (considerable restrictions apply), monopolistic (usually related to the uniqueness of goods)	Monopolistic, imperfect competition, self-regulated, overpriced goods	Monopolistic, imperfect competition, self-regulated, overpriced goods
Competition protection	State-level protection by law	None	None
Activity outcome	Legal goods and services	Illegal goods and services	Illegal informational goods and services
Subjects	• Private persons • State	• Private persons • State	• Private persons • State
Objects	• Private persons • State	• Private persons • State	• Private persons • State
Types	• Profit • Non-profit	• Profit	• Profit
Interest	• Profit • Public service	• Profit	• Profit
Goods	• Private goods	• Weaponry	• Specialized

	• Common goods • Club goods • Public goods	• Drugs • Human traffic • Illegally logged timber • Animals and animal products • Alcohol • Tobacco • Biological organs • Currency • Fuel • Counterfeit medicine, essential aircraft and automobile parts	software • Spyware devices • Card counterfeiting equipment • Pirated software • Private data • Software and hardware vulnerabilities
Services	• Business functions • Childcare • Clear, repair and maintenance • Construction • Dispute resolution • Education • Entertainment • Financial services • Foodservice • Health care • Hospitality industry • Information services • Risk management • Social services • Transport • Public utility • Etc.	• Human traffic • Racketeering • Transportation providers	• Analytics • Social Engineering • Spam • Phasing • Pharming • Extortion • Sabotage • Terrorism • Piracy • Proxy services rent • DoS attacks • Botnet creation and rent • Money laundering
Employment	Official	Unofficial, unaccounted	Unofficial, unaccounted

One of the major differences between the three is the employed goods and services. In the domain of information technologies, goods and services may often be confused due to their intangibility.

Goods in economics often refer to something intended to satisfy consumer needs. Goods are often considered to be tangible, while in the domain of information technologies only computer hardware is tangible. The most common criminal information technologies goods are the following ones:

- Specialized software – even though a lot of software in this category may be created with good intentions such as penetration testing for information security professionals in mind, these tools may be often used without proper authorization and for malicious purposes.
- Spyware devices – credit card skimmers, electromagnetic impulse readers, hardware keyloggers, etc.
- Card counterfeiting equipment – fake plastic card producing and copying equipment.
- Pirated software – a major profit loss as is being claimed by software manufacturers.
- Private data – stolen logins, e-mails, passwords, credit card data, and all of the possible data, that may be used in identity fraud.
- Software and hardware vulnerabilities – according to Rainer Boehme and his paper named Vulnerability Markets, a stable and well-formed market of vulnerabilities exists. The researcher defines five types of vulnerability markets: bug challenges, bug auctions, vulnerability brokers, exploit derivatives, and cyber insurance.

Among the most common criminal information technologies services we would like to outline the following ones:

- Analytics – software vulnerabilities analysis, reverse-engineering, market and legislation analysis.
- Social Engineering – a method of acquiring personal data via winning one's confidence pretending to be a person that victim would normally trust.
- Spam – unsolicited advertisement delivery. Even though anti-spam techniques have substantially evolved during past years, undesirable messages still get through sometimes, which is annoying to users and may sometimes cause mailing systems malfunction.
- Pharming – attack via redirecting end user's web traffic from a legitimate web-site to a malicious one.
- Phishing – attack aimed at acquiring personal data via tricking user into entering his personal data (such as login information, passwords, e-mails, credit card data) on a malicious web-site pretending to be legitimate one, which the user would normally trust.
- Extortion – being very similar to real-world extortion, its virtual-world counterpart aims at rendering some of the user's hardware useless unless a certain amount of money is paid. It is not unusual that even after the sum is transferred, malware continues to extort.
- Sabotage – deliberate action aiming at causing system malfunction.
- Terrorism – it is difficult to provide an unambiguous definition of this term, but, generally, a terrorist is a person who uses violence and coercion as means of reaching his or her goals. When speaking of terrorism in the domain of information technologies, one would often imply DoS attacks, web-site defacing, sabotage, specialized malware. Hacktivism may also fall into this category, even though it is usually much less harmful.
- Piracy – a service aiming at copyright infringement via unauthorized software copying, distribution, etc.
- Proxy services rent – a large proxy network may be often used to prevent malefactor's physical detection while sending patches and commands to botnets.
- DoS attacks – often sold as a service to those who don't have enough resources to perform it on their own.

- Botnet creation and rent – botnets may be widely used for DoS attacks, spamming, as proxies, etc.
- Money laundering – by means of information technologies. It is noteworthy that not only money earned in criminal sector of information technologies may be laundered this way. And after being laundered it may be used to further elaborate and develop both cyber and real-life crime.

5. Conclusion

The authors are aware of the complexity and complicacy of the issues brought up in this article, and realize that no quick solutions are available. Heightened interest to this subject gives hope for a successful resolution of the problems, but many issues are still left unresolved.

We find it important to draw researchers' attention to the following question, which requires immediate attention: What is the solution to the problem of shadow information economics? How is it possible to defeat it? Is it possible to completely annihilate it? Probably, not. Is it possible to lead all the shadow entities out the underground? One might suggest using the stick and carrot policy, punishing everyone who doesn't, and stimulate those who do. Or should we try and create the circumstances, where being in the shadow would be economically disadvantageous?

References

1. Spy Ops, Technolytics, Intelomics. *Cyber Weapons Threat Matrix*, http://spy-ops.com/web/CyberWeapons_Threat_Matrix.pdf
2. Symantec, *State of Information Global Results*, 2012, http://www.symantec.com/content/en/us/about/media/pdfs/2012-state-of-information-global.en-us.pdf
3. Digital Forensics Association, *The Leaking Vault 2011 Six Years of Data Breaches*, 2011, http://www.digitalforensicsassociation.org/storage/The_Leaking_Vault_2011-Six_Years_of_Data_Breaches.pdf
4. Andy Greenberg, Forbes. *Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits*, http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/
5. Boehme, Rainer. *Vulnerability Markets. What is the economic value of a zero-day exploit?* http://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf
6. Raj Samani, McAfee. *Cybercrime Exposed, Cybercrime-as-a-Service* http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-exposed.pdf
7. Symantec Corporation. *Internet Security Threat Report 2013*, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf