PARTEA TENEBRĂ A ECONOMIEI INFORMAȚIONALE

Drd. Grigori BORTA, ASEM

Este greu de imaginat lumea modernă fără tehnologiile informaționale, acestea fiind utilizate la nivelurile locale, corporative, naționale și internaționale. Cu toate acestea, în pofida multor beneficii pe care le oferă, numeroasele tehnologii informaționale pot fi folosite atât în scopuri negative, cât și pozitive. Uneori, utilizatorii sunt dispuși să-și sacrifice siguranța datelor personale de dragul comodității.

Prejudiciul generat de existența acestui domeniu este evident. De exemplu, conform datelor Biroului Federal de Investigații (Federal Bureau of Iinvestigation – FBI), pe parcursul ultimelor 14 luni, atacatorii au sustras aproximativ 215 milioane de dolari SUA, utilizând o singură schemă frauduloasă, asociată cu adresele de e-mail corporative compromițătoare. Totalul victimelor a constituit 2126 de persoane, printre care se numără 1198 de cetățeni americani și 928 de cetățeni din alte țări. Este remarcabil faptul că cetățenii Statelor Unite au suferit daune mult mai considerabile, în valoare totală de aproximativ 180 de milioane dolari SUA, ce au reprezentat circa 84% din totalul pierderilor.

Cuvinte-cheie: *economie informațională tenebră, securitatea informației*

JEL: D82, L86, M15

Introducere

Scopul articolului acesta constă în încercarea de a atrage atenția asupra problemei economiei informaționale tenebre. Efectul negativ a existenței sectorului dat este evident: de exemplu, pagubele susținute de către Banca Heartland cauzat de vulnerabilitatea în sistemul de securitate, sunt estimate de către experți în jur de 12,6 milioane dolari SUA. Cu excepția cheltuielilor evidente, precum ar fi eliminarea vulnerabilității ce a cauzat pagube, marea parte a cheltuielilor este constituită din plăți către clienții companiei și pierderea clienților existenți și potențiali, ce duce la pierderea profitului pe termen lung. Conform cercetării publicate în revista „Washington Post", desfășurată în anul 2006, referitoare la reprezentanții serviciilor oficiale, au fost înregistrate daune în jur de 250 miliarde de dolari, cauzate de materialele ce încalcă drepturile de autor. Business Software Alliance citează cifre mai mici, afirmând că volumul pieței producției piratate a crescut de la 58.8 miliarde dolari SUA, în 2010, până la 63 miliarde, în 2011. Toate acțiunile menționate aparțin economiei informaționale tenebre.

Definirea economiei informaționale tenebre

Economia informațională tenebră (EIT) este

THE DARK SIDE OF INFORMATION ECONOMICS

PhD candidate, Grigori BORTA, ASEM

It is difficult to imagine modern world without information technologies. They are widely used on domestic, corporate, state and international levels. But even though these technologies offer multiple benefits, they can be used for both good and bad. Sometimes, users are eager to sacrifice security of their personal data for the sake of convenience.

The damage of this domain's existence is obvious. For example, according to the data provided by FBI, during the last 14 months, malefactors have stolen around 215 million US dollars using just a single scam, related to compromised corporate e-mail addresses. 1198 of the victims were US citizens, and 928 citizens of the other countries, thus totalling the number of victims to 2126. It is important to note, that US citizens suffered much more damage, totalling 180 million US dollars, or in other words, 84% of total damage done.

Key words: *shadow information Economics, information security*

JEL: D82, L86, M15

Introduction

This paper aims at drawing attention to the problem of the shadow domain of information Economics. The negative impact of the sector's existence is obvious: for example, damage done to Heartland Bank due to a security breach is estimated by experts to be around USD 12.6 million. Apart from the obvious expenses aimed at eliminating the vulnerability, a lot of money will be spent on client payoffs; a lot of existing and potential clients will consider choosing a different bank which will certainly cause loss of profit in the long term. According to a research published in Washington Post in 2006, referencing the officials, damage done by copyright law infringement is estimated around USD 250 billion. Business Software Alliance claimed that the damage is less, and probably around USD 58.8 billion in 2010, and around USD 63 billion in 2011. All of the abovementioned actions are a part of shadow information Economics.

The definition of shadow information Economics

Shadow information Economics – is a specific sphere of economic activity with a distinct structure and system of economic relations. The specifics are demonstrated by illegality, informality, criminal character of economic activity and income concealment [8].

domeniul specific de activitate economică, cu structura şi sistemul de relaţii economice inerente. Specificitatea acesteia este determinată de caracterul ilegal, neoficial, precum şi cel penal al activităţii economice şi disimularea veniturilor.

Economia informaţională tenebră reprezintă sectorul relaţiilor economice, ce acoperă toate tipurile activităţii comercial-industriale, care, după direcţia, conţinutul, natura şi forma sa, contravin cerinţelor legislaţiei în vigoare şi sunt aplicate în pofida reglementării economice guvernamentale prezente.

Economia informaţională tenebră prezintă activităţile individuale şi colective ilegale, legate de proiectarea, dezvoltarea, distribuţia, susţinerea şi utilizarea componentelor tehnologiilor informaţionale şi comunicaţionale, ascunse de societate. Asemănarea dintre economia tenebră şi EIT este reflectată prin similitudinea caracteristicilor, funcţiilor şi descrierilor.

Trăsăturile caracteristice ale economiei informaţionale tenebre sunt:

- caracterul ascuns;
- implicarea tuturor fazelor procesului de reproducţie socială.

S-ar părea că acest domeniu este foarte apropiat economiei tenebre clasice, însă, cu toate acestea, are o serie de deosebiri semnificative şi foarte importante, precum:

- natura intangibilă a majorităţii bunurilor şi serviciilor;
- virtualitatea tuturor relaţiilor existente pe piaţa dată.

Analiza premiselor şi istoriei de evoluţie a economiei informaţionale tenebre

Se disting trei etape de bază ale formării economiei informaţionale tenebre:

- Pre-calculator – se caracterizează prin apariţia premiselor pentru dezvoltarea economiei informaţionale tenebre: dezvoltarea sistemului juridic, economic şi financiar, aparenţa primelor prototipuri ale tehnicii de calcul. Majoritatea statelor se confruntă atât cu problema economiei tenebre „clasice", cât şi cu cea informaţională.
- Timpurie – această etapă este asociată cu o accelerare semnificativă a ritmurilor de dezvoltare a tehnologiilor computerizate, precum şi cu apariţia specialiştilor în acest domeniu. În acest stadiu, apare primul software malițios, care poartă, în mod principal, un caracter de cercetare sau distructiv (de exemplu, viermele Morris).
- Modernă – etapa respectivă se caracterizează printr-o tendinţă a unificării atacatorilor în grupuri, unde fiecare membru joacă un rol extrem de specializat. Sarcinile lor pot varia de la cercetarea software-ului şi hardware-

Shadow information Economics is the domain of economic relationships, covering all the production and economic activity that in their form and character contradict the requirements of existing law and are performed in defiance of state regulation of economy and surpassing existing controls.

Shadow information Economics is the entire individual and collective activity that is illegal, related to design, development, spread, support, and use of all the components of information and communication technologies, and is concealed from society. Similarities between "regular" and shadow information Economics consist of resemblances in their characteristics, functions, and descriptions.

Shadow information Economics is characterized by the following features:

- concealed character,
- all the phases of economic reproduction are encompassed.

It may seem that this domain is very similar to "classic" shadow Economics, but there is a number of very important distinctions:

- intangibility of the majority of goods and services,
- virtuality of all the relationships existing in this market.

Analysing the premises and the history of shadow information Economics

Three major stages of shadow information Economics formation are defined:

- Pre-computer – characterized by the origins of premises for the development of shadow information Economics: law, economical, and financial systems are formed, first computer prototypes appear. The vast majority of countries encounter the problem of both "classical" and shadow information Economics.
- Early – this stage is characterized by considerable increase in the progress of computer engineering, as well as by appearance of specialists in the domain. First malware is spotted during this period, which bears, for the most part, academic or destructive purpose (e.g. Morris worm).
- Modern – characterized by the tendency of malefactors to form groups, where each individual performs a very narrow task. Such tasks may include the following: analysing hardware and software, market, law, possible ways of money laundering, etc. Many of the specialists who were hackers during the previous stage now become cyber security experts. Such

ului pieței, legislației, până la găsirea unor posibilități de spălare de bani etc. Mulți experți, foști hackeri ai etapei incipiente de dezvoltare a economiei informaționale tenebre, în acest stadiu, devin specialiști în securitatea informațională. În această etapă, apar astfel de noțiuni, precum: arme cibernetice, războiul cibernetic (Stuxnet, DuQu, Flame). O altă trăsătură caracteristică prezintă epidemiile frecvente de viruși și creșterea volumului software-ului piratat (ZeuS, Conficker). O popularitate, tot mai mare, o dobândesc și tehnologiile de tip „cloud".

Analiza structurii economiei informaționale tenebre

Trăsătura distinctă a structurii economiei informaționale tenebre este dictată de intangibilitatea majorității produselor implicate. Se evidențiază două segmente principale de pe piața economiei informaționale tenebre: produse și servicii. În continuare, analizăm fiecare dintre acestea în detaliu.

Produse în sfera economiei informaționale tenebre

Sub cuvântul „produs" putem să înțelegem un obiect, care poate să satisfacă nevoile specifice și în mai multe cazuri este material. Totuși, după cum a fost specificat mai devreme, în sfera informațională, totalitatea componentelor fizice ale unui calculator poate fi atribuită hardwae-ul, alte produse comportă mai mult un caracter intangibil. Putem să deosebim următoarele produse, care sunt folosite în această sferă:

- Software-ul specializat. În categoria dată, se află Adware, spyware, crimeware, viruși, generatori de software malware, exploit, viermi, troieni, scareware, aplicații potențial nedorite, rootkits, packere, script-uri redirecționării traficului.
- Spyware-ul hardware. De exemplu, keylogger-ul, interceptează dispozitivele de comunicații fără fir.
- Materialele prin care se încalcă drepturile de autor, de asemenea, numite piraterie.
- Materialele și software-ul prin care se încalcă Acordul de Utilizare.
- Aparatele și instrumentele pentru fraudarea cardurilor de plată, așa-numitul „carding".
- Vulnerabilitățile în software și hardware.
- Datele personale.
- Armele cibernetice. Acest termen se aplică unor astfel de programe malware, ca Stuxnet, DuQu, Flame, Gauss, după părerea mai multor cercetători, produse similare puteau fi proiectate de reprezentanții guvernului.

notions as hacktivism, cyber weaponry, cyber war (Stuxnet, DuQu, Flame) appear during this period. Other major trends are the increase in computer virus epidemics (ZeuS, Conficker) and in software pirating. Cloud technologies start gaining popularity.

Shadow information Economics structure analysis

Particularity of shadow information Economics is demonstrated by intangibility of the most part of the goods involved in it [1]. This is for the most part caused by intangibility of the majority of goods and services represented in this market [6]. Exactly this factor is the major one, when defining the differences between shadow information Economics and its "classic" counterpart. A definitive border cannot be always traced because of constant changes in this domain, its universal character, and its rapid and constant development. Two most important segments are outlined in the market of shadow information Economics: goods and services. They are analysed in more detail further.

Goods in the domain of shadow information Economics

A good is something aimed at satisfying the needs of a consumer and that is usually tangible. But as was mentioned earlier, the goods in the information domain usually bear intangible character, only hardware being tangible. The following major categories of goods are outlined as being the most representative parts of shadow information Economics:

- Specialized software. Adware, spyware (in its software form), crimeware, computer viruses, malware generators, worms, exploits, Trojan horses, scareware, potentially unwanted software, rootkits, executable packers, and TDSs belong to this category.
- Spyware (in its hardware form). For example, key loggers, wireless communication loggers, etc.
- Pirated materials.
- Software and other materials, violating end-user agreement.
- Hardware and the tools used for credit card forgery, so called carding.
- Software and hardware vulnerabilities [2][3].
- Personal data, for example, credit card data, e-mail passwords, etc.
- Cyber weaponry. This term is applied to software like Stuxnet, DuQu, Flame, Gauss because many of the researchers studying the subject affirm that this kind of software could only be developed by governmental structures.

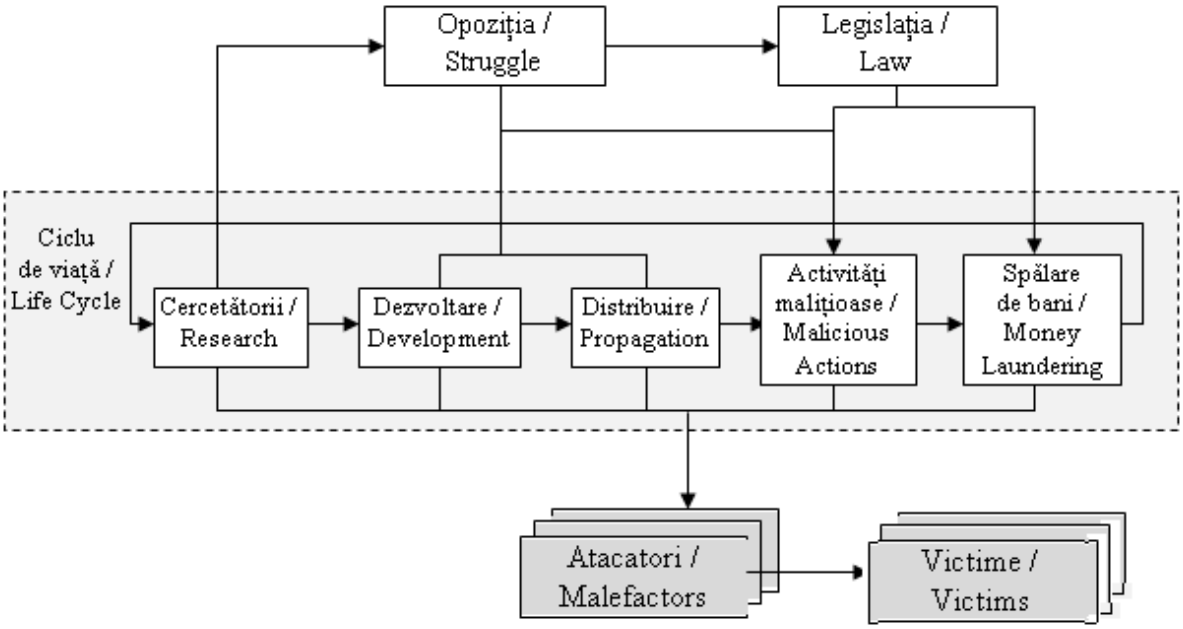

Figura 1. Structura procesului de reproducere pe piața tenebră a tehnologiilor informaționale / Figure 1. The structure of the process of reproduction in the shadow information technologies market

Servicii în sfera economiei informaționale tenebre

Serviciile sunt atât de strâns legate de produse, din care cauză, de multe ori, este imposibil de a trage o linie clară între aceste două categorii. În sfera informațională tenebră, pot fi evidențiate următoarele categorii de servicii dubioase:

- Analitice
- Furtul datelor personale
- Închirierea softului
- Phishing
- Farming
- Extorcare
- „Scrisorile Nigeriene”
- Sabotaj
- Terorism
- Piraterie
- Închiriere a serverelor proxy
- Spălarea banilor prin utilizarea informației tehnologice
- Crearea şi închirierea botneturilor
- DoS atacurile
- Spam-ul
- Producerea cartelelor de credit contrafăcute („carding”)

Monetizarea

Există mai multe scheme de monetizare a produselor şi a serviciilor în sectorul tenebru al tehnologiei informaționale:

- PPI – Plata pentru instalare la calculatorul victimei a unui software dăunător. De obicei, atacatorul infectează un calculator cu așa-

Services in the domain of shadow information Economics

The services category is so deeply intertwined with the products category, that it is very often impossible to draw a clear border between them. The following major service types are defined in the domain of shadow information Economics:

- Analytics,
- Personal data theft
- Software renting
- Phishing
- Pharming
- Extortion
- “Nigerian scam”
- Sabotage
- Terrorism
- Piracy
- Proxy servers rent
- Money laundering using information technologies
- Creation and rent of bot-nets
- DoS-attacks
- Spam
- Carding

Monetization

A couple ways of monetizing goods and services in the shadow domain of information Economics exist:

- PPI – pay-per-install. The payment for installing malware on victim’s computer. Usually the malefactor starts with infecting the victim’s computer with a so called

numitul Dropper, care, ulterior, este utilizat pentru instalarea altor software dăunătoare. Plata este efectuată pentru fiecare instalație a programului la fiecare calculator.

- Vânzarea – vulnerabilitatea este la mare căutare pe piața neagră a tehnologiilor informaționale. Pe lângă programe care oferă recompense pentru vulnerabilitățile software-lui, care sunt organizate de către programatorii oficiali, există pe piața neagră vulnerabilități, la care se oferă adesea mult mai mari recompense.
- Dropul – cumpărături în magazinele online și livrare a acestora printr-un lanț de intermediari, de asemenea, cunoscut sub numele de „catâri".
- Offshore – efectuarea plăților prin zonele off-shore. Este dificil de a urmări originea unor astfel de plăți.
- Plățile directe – achizițiile efectuate de către victime, de exemplu, promisiunea de a decripta fișiere, criptate cu ajutorul malware software sau taxe de licență pentru activarea anti-virusului fals.
- Furnizarea serviciilor, cum ar fi trimiterea spamului, serviciului proxy.

Concluzie

Materialul prezentat nu este o descriere exhaustivă a economiei informaționale tenebre, structurii ei și proceselor care au loc în acest domeniu. Este necesar un studiu cuprinzător și aprofundat al structurii în sine a economiei informaționale tenebre, precum și o analiză a dezvoltării mecanismelor și procedurilor, care pot să facă față la toate vulnerabilitățile apărute la etapele ciclului de viață ale software și hardware. Concomitent, trebuie dezvoltate și implementate mijloace legale, instituționale și economice eficiente pentru combaterea sectorului tenebru al economiei informaționale.

"downloader" malware which is later used to install further malicious software. The payment is then made for each malware installation on each of the victims' computers.

- Sales – vulnerabilities are in great demand on the shadow information market. Besides the official programs that offer rewards for bugs and vulnerabilities there is a huge shadow market for vulnerabilities, which usually offers much higher rewards.
- Drop – buying goods on the Internet and their delivery via a chain of intermediaries, also known as "mules".
- Offshore – all the payments are made through the offshore zones. This complicates the process of tracking the origins of this kind of payments.
- Direct payments – purchases made by the victims in return for a promise of deciphering their documents, encrypted with malicious software or direct payments for the scareware "license".
- Services, such as spam, proxy servers, etc.

Conclusion

The presented material is by no means a comprehensive description of shadow information Economics, its structure or the processes taking place. A much more complex and profound research of its structure is required in order to establish effective mechanisms and procedures aimed at the struggle against each stage of each software and hardware vulnerability's life cycle. Effective law, organizational, and economical measures of struggle against shadow sector of information Economics must be developed and implemented. A set of corrections to the existing law should be developed and introduced, that will be aimed at the struggle against both general shadow information Economics and offences in this domain.

Bibliografie / Bibliography:

1. SCHNEIER, Friedrich și KEPLER, Johannes. *The Shadow Economy in Europe 2013*. 2013.http://www.protisiviekonomiji.si/fileadmin/dokumenti/si/projekti/2013/siva_ekonomija/The_Shadow_Economy_in_Europe_2013.pdf.
2. ZORZ, Zeljka. *How much does a 0-day vulnerability cost*? Help Net Security. Vizitat la 26 martie 2012. http://www.net-security.org/secworld.php?id=12652.
3. SCHNEIER, Bruce. *The Vulnerabilities Market and the Future of Security*. Forbes. 30 mai 2012. http://www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/.
4. PERLROTH, Nicole, SANGER, David E. *Nations Buying as Hackers Sell Flaws in Computer Code*. The New York Times. 13 iulie 2013. http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?_r=0.
5. VALENTINO-DEVRIES, Jennifer; SONNE, Paul; MALAS, Nour. *U.S. Firm Acknowledges Syria Uses Its Gear to Block Web*. The Wall Street Journal. 29 octombrie 2011. http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html.

6. CHIESA, Raoul. *Cybercrime & underground economy: operating and business model*. Flare Network. 1 iulie 2010. http://www.flarenetwork.org/report/enquiries/article/cybercrime_and_underground_economy_operating_and_business_model.htm.
7. KREBS, Brian. *FBI: Businesses Lost $215M to Email Scams*. Krebs on Security. Vizitat la 28 ianuarie 2010. http://www.krebsonsecurity.com/2015/01/fbi-businesses-lost-215m-to-email-scams/.
8. OHRIMENCO, Serghei, SARKISIAN, Agop, BORTA, Grigori. *Price policy model at the modern shadow market of information technologies*. International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE-2012). October 5 – 6th, 2012 University of National and World Economy. Sofia, Bulgaria.