SECURITATEA NAȚIONALĂ ŞI DIMINUAREA RISCURILOR CIBERAMENINȚĂRILOR

Elena BĂDĂRĂU[1], prof., IRIM

În ultimul timp, asistăm la un atac concertat asupra creanțelor comerciale, care îşi desfăşoară activitatea prin intermediul internetului. De asemenea, asistăm, la o creştere alarmantă a tentativelor de fraudă prin internet îndreptate asupra băncilor comerciale. Dacă ar fi să vorbim la modul figurat, escrocii merg la pescuit de clienți naivi. Cunoscut sub numele de phishing, fenomenul reflectă pe deplin modul de operare, ideea de bază fiind aruncarea momelii şi prinderea în cârlig a clienților lipsiți de prevedere. Când utilizatorul obişnuit de colculator aude cuvântul "hacker", cei mai mulți cred că este vorba despre un criminal dubios de Internet care va sparge dosarele secrete de stat sau va fura identitatea persoanelor şi informațiile cardului de credit.

Cu toate acestea, pentru tehnicieni termenul nu se limitează doar la oamenii care folosesc capacitățile lor profesionale în scop de crimă. Prin "hackeri" se subînțeleg experți în informatică care pot crea/modifica codul la calculator şi intra nedetectați în sistemele informatice. Hackerii, în funcție de intențiile lor, pot fi împărțiți în trei categorii: hackeri-pălărie albă: hackeri non-malware, cum ar fi angajații firmei care testează securitatea sistemului propriu de calculatoare, încercând să pătrundă în ele. Hackeri-pălărie neagră/ biscuiti: hackeri cunoscuți, de asemenea, sub numele de „crackers", care intră în sisteme cu intenția de a fura sau vandaliza. Hackerii pălărie gri: ei se plasează între „pălărie albă" şi „pălărie neagră", sunt cei care uneori acționează ilegal. Ei pot pătrunde, de exemplu, în sistem, fără autorizație, în scopul de a depista vulnerabilitățile şi apoi cerând proprietarului să achite o taxă pentru scenariul de înlăturare a problemei. Cuvântul "hackeri", utilizat în sensul de calculator, a apărut pentru prima dată în anul 1963, în MIT (Massachusetts Institute of Technology) „The Tech". Acesta a fost folosit pentru a descrie farse cu implicarea tehnologiei. Membrii MIT „The Tech" au început să aplice argoul modelului de cale ferată la un calculator. MIT „The Tech" a devenit sediul-bază pentru primii hackeri şi experimentele lor. La începutul anilor '70-80, termenul "hacker" a fost folosit pentru a descrie un programator vizionar, pasionat de a veni cu noi moduri de a folosi un calculator – crearea de noi programe şi sisteme. Directori ai companiilor de Calculatoare, precum Steve Jobs, Steve Wozniak şi Bill Gates au fost toți hackeri din al doilea val. Astăzi, expresia este folosită mai degrabă pentru persoanele care intră în sisteme şi lucrează cu codul, decât cu referire la creatorii de software. Pe site-ul BullGuard veți vedea de multe ori sintagma "criminali de internet", ca un termen-umbrelă care acoperă oamenii ce încearcă de a proteja utilizatorul obişnuit de astăzi.

La început de mileniu, accesul la internet la domiciliu a devenit o marfă obişnuită şi cu extindere spre noi posibilități practice online, cum ar fi serviciile bancare online şi

NATIONAL SECURITY & REDUCING OF CYBER-ATTACK RISKS

Elena BADARAU, prof., IRIM

When ordinary computer user hears the word "hacker", most think of a dodgy internet criminal who breaks in to government intelligence files or steal people's identities and credit card information. For the more tech savvy, however, the term is not just limited to people who use their ability for crime. By "hackers" they mean computer experts who can create and alter computer code and enter computer systems undetected. Hackers can be divided into 3 head categories depending on their intentions: White hat hackers: non-malicious hackers, like company employees who test the security of the firm's own computer system by trying to break into it. Black hat hackers/crackers: malicious hackers, also known as crackers, who hack into systems with the intent to steal or vandalize. Grey hat hackers: in between the white hat and the black hat hacker, grey hats sometimes act illegally. They will for example break through a system without authorization in order to put vulnerabilities on show and then charge the owner a fee to repair it. The word "hackers" used in the computer sense appeared for the first time in 1963 in the MIT (Massachusetts Institute of Technology) paper "The Tech". It was used to describe pranks involving technology. Members of MIT's Tech Model Railroad Club had begun working with a computer and started applying the model railroad slang to computers. MIT became the building ground for the very first computer hackers and their experiments. In the early days, the 70's and 80's, the term "hacker" was used to describe a visionary programmer, passionate about coming up with new ways to use a computer – building new programs and systems. Computer company executives like Steve Jobs, Steve Wozniak and Bill Gates were all hackers back in the day. Today, the phrase is used more about individuals who enter systems and work with code, rather than with reference to software creators. Here on the BullGuard website you will often see the phrase "internet criminals", as an umbrella-term covering the people we try to protect the ordinary user from today. At the turn of the millennium, internet access at home was becoming a normal commodity and with this followed new practical online possibilities like online banking and shopping. Useful as the new possibilities were, they also opened the door for a part of the underground community of hackers, virus writers etc. to take their activities to the next level and make money off their illegal hobbies. This was the case for some, while others put their abilities to good use by working for companies or governments. The days when virus creators spread out infections with the purpose of making a name for themselves are gone. Nowadays cybercrime is better organized than ever and is becoming a multimillion dollar "business". Moreover, the increasing popularity of social networking sites has attracted the attention of cyber criminals which exploit these in every possible way gaining significant financial benefits. Cyber fraud caused by Internet criminals accounts for

[1] ***© Elena BĂDĂRĂU, el.badarau@gmail.com***

cumpărături online. Noile comodităţi au deschis, de asemenea, uşa pentru o parte a comunităţii tenebre de hackeri, care reuşesc să facă bani de pe hobby-urile lor ilegale.

Cuvinte cheie: *afaceri, e-comerţ, e-gov, securitate.*

approximately 60 million pounds in UK only and it is likely to move away from home users and concentrate on companies targeting larger amounts of money.

Key words: *business, e-commerce, e-gov, security.*

JEL Classification: F52, F23, F1, F59, G3

Introducere. Ţările lumii, inclusiv R.Moldova sunt lideri după numărul de atacuri ciberfinanciare prin intermediul programelor soft periculoase.

Internetul este suprasaturat de programe periculoase având ca scop conturile bancare şi moneda electronică. Nivelul riscurilor financiare în ultimul an a crescut semnificativ.

Conform datelor obţinute în 2013, numărul de atacuri de orientare financiară, chiar atacuri de tip phishing sau cu folosirea de software periculoase, este de asemenea în creştere.

Software periculoase

- Numărul atacurilor cibernetice, folosind malware, care vizează furtul de date financiare, în 2013 a crescut cu 27,6%, ajungând la 28,4 mil. Numărul de utilizatori atacaţi a crescut atingând cifra de 3,8 mil persoane – o creştere anuală de 18,6%.

- Ponderea utilizatorilor care au fost atacaţi financiar prin utilizarea programelor periculoase în 2013 a ajuns la 6,2% din numărul total de atacuri. Comparativ cu anul 2012, cifra a crescut cu 1,3%.

Printre programele periculoase pentru fraude financiare cel mai activ s-au utilizat instrumentele vizând Cryptovaluta Bitcoin. Cu toate acestea, el joacă rolul dominant în fraude financiare din conturile bancare, cum ar fi programul Zeus.

Introduction. Some countries, including Moldova are leaders by number of financial cyber-attacks by dangerous software programs.

The Internet is replete of malware aimed at the bank accounts and electronic money. The level of financial risk has increased significantly in the last year.

According to the data from 2013, the number of attacks targeting financial, even phishing attacks or the use of malicious software has increased notably.

Dangerous Software

- The number of cyber attacks using malware aimed at stealing financial data in 2013 increased from 27.6% to 28.4 million. The number of users increased to 3.8 million attacked people with an annual increase of 18,6%.

- The share of users that were attacked financially by using of malicious programs in 2013 reached 6.2% of the total number of attacks. Compared with 2012, the figure has increased by 1.3%.

Among the threats to the most active financial fraud were used instruments aimed at Crypto currency Bitcoin. However, it plays the dominant role in financial fraud bank accounts, such as Zeus program.

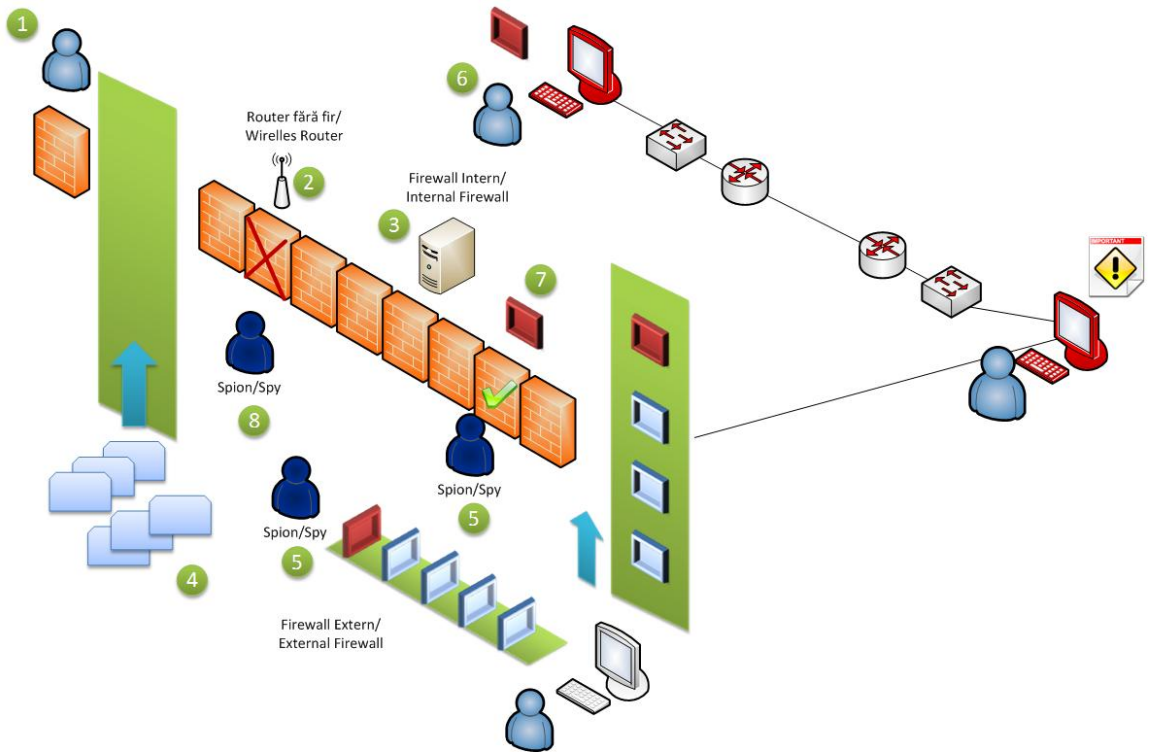

Fig. 1. Penetrarea unei reţele de calculatoare/
Fig. 1. Penetration of computer networks

Fiind un domeniu complex, au fost create domenii de diviziune pentru a putea face administrarea mai facilă. Această

As a complex domain, division areas were created in order to make administration easier. This division allows

împărțire permite profesioniştilor o abordare mai precisă în privința instruirii, cercetării şi diviziuni muncii în acest domeniu. Sunt 12 domenii ale securității rețelelor specificate de International Organization for Standardization (ISO)/ International Electrotechnical Commission(IEC):

1. **Evaluarea Riscului** e primul pas în administrarea riscului şi determină valoarea cantitativă şi calitativă a riscului legat de o situație specifică sau o amenințare cunoscută;
2. **Politica de Securitate** este un document care tratează măsurile coercitive şi comportamentul membrilor unei organizații şi specifică cum vor fi accesate datele, ce date sunt accesibile şi cui;
3. **Organizarea Securității Informației** este un model de guvernare elaborat de o organizatie pentru securitatea informației;
4. **Administrarea Bunurilor** reprezintă un inventar potrivit unei scheme clasificate pentru bunurile informaționale;
5. **Securitatea Resurselor Umane** definește procedurile de securitate privind angajarea, detaşarea şi părăsirea de către un angajat a organizației din care va face, face sau a făcut parte;
6. **Securitatea Fizică şi a Mediului** descrie măsurile de protectie pentru centrele de date din cadrul unei organizații ;
7. **Administrarea Comunicațiilor şi Operațiunilor** descrie controalele de securitate pentru rețele şi sisteme;
8. **Controlul Accesului** privește restricțiile aplicate accesului direct la rețea, sisteme, aplicații şi date;
9. **Achiziția, Dezvoltarea şi Păstrarea Sistemelor Informatice** definește aplicarea măsurilor de securitate în aplicații;
10. **Administrarea Incidentelor de Securitate a Informației** tratează cum anticipează şi răspunde sistemul la breşele de securitate;
11. **Administrarea Continuității Afacerii** descrie măsurile de protecție, întreținere şi recuperare a proceselor critice pentru afacere şi sisteme;
12. **Conformitatea** descrie procesul de asigurare a conformității cu politicile de securitate a informației, standarde şi reguli.

Aceste 12 domenii au fost create pentru a servi ca bază comună pentru dezvoltarea de standarde şi practici de securitate eficientă şi pentru a da încredere activităților desfăşurate între organizații.

Tot pe criterii de eficiență în abordare şi usurință în învățare, atacurile de securitate la adresa rețelelor sunt împărțite cu carater general în: recunoaştere, acces şi imposibilitate de onorare a cererii (DoS).

Malware-ul Mobil

▪ În colecția „Kaspersky Lab" numărul de aplicații malware pentru Android – concepute pentru a fura datele financiare, a crescut în a doua jumătate a anului 2013 de aproape 5 ori, de la 265 modele în luna iunie, pînă la 1 321 - în luna decembrie.

▪ În anul 2013 experții „Kaspersky Lab" au descoperit primul troian pentru Android, care putea fura bani din conturile bancare ale utilizatorilor.

Malware-ul financiar

Programele de furt a banilor electronici şi a informațiilor financiare sînt unele dintre cele mai complexe şi dificile tipuri de malware. Această clasă de programe permite infractorilor cibernetici de a converti rapid eforturile lor în venituri, astfel încît acești atacatori nu cruță nici eforturile nici resursele pentru

the professionals a more precise approach regarding education, research and division of labor in this area. There are 12 areas of network security specified by the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC):

1. **Risk assessment** is the first step in risk management and determines the quantitative and qualitative risks in a specific situation or a known threat;
2. **Security policy** is a document that deals with enforcement action and behavior of members of an organization and specifies how data will be accessed, what data are available and to whom;
3. **Organization of Information Security** is a governance model developed by an organization for information security
4. **Asset Management** is an inventory that accords to a classified scheme for information assets.
5. **Safety Human Resources** defines security procedures on hiring, posting and leaving by an employee of the organization they will do, or having been part of.
6. **Physical and Environmental Security** describes the protection measures for data centers within an organization.
7. **Communications and Operations Administration** describes network security controls and systems
8. **Access Control** concerns restrictions applied to direct access to the network, systems, applications and data.
9. **Acquisition, Development and Retention of Information Systems** defines the security controls in applications
10. **Security Incident Information Management** deals with how the system anticipates and responds to security breaches
11. **Business Continuity Management** describes protection, measures, maintenance and recovery of critical business processes and systems
12. **Compliance** describes the process of compliance with information security policies, standards and rules.

These 12 areas have been created to serve as a common basis for developing effective security standards and practices and to give confidence activities between organizations.

Also on efficiency criteria in approach and ease of learning, security attacks against networks are divided into broad picture: recognition, access and honoring impossible demand (DoS).

Mobile malware

● The number of malicious Android-applications in "Kaspersky Lab" collection designed to steal financial data increased by almost 5 times, with 265 samples in June to 1321 in December.

● The "Kaspersky Lab" experts has discovered Trojan for Android, that can steal money from attacked users' bank accounts.

Financial Malware

Programs for theft of electronic money and financial information is one of the most difficult types of malware. This class of programs allow cybercriminals to convert their efforts into income quickly, so attackers do not spare efforts and resources on the creation of financial Trojans and backdoors. According to observations of

crearea troienilor financiari şi a backdoor-urilor. Potrivit observaţiilor experţilor „Kaspersky Lab", autorii de malware sunt dispuşi să plătească zeci de mii de dolari pentru informaţii despre noile vulnerabilităţi, numai pentru a ocoli produsele securizate şi pentru a depăşi concurenţa "pieţei negre".

În 2013 „Kaspersky Lab" a denunţat 28,4 mln de atacuri financiare malware, fiind cu 27,6% mai mare decît în anul anterior. Numărul de utilizatori atacaţi de un malware similar de asemenea a crescut cu 18,6% - până la 3,8 mln. În acest studiu a fost inclusă şi baza datelor privind atacurile cu ajutorul programelor bancare troiene, keyloggerilor, software-ul pentru furtul portofelelor virtuale Bitcoin şi programe de descărcare pentru a genera această monedă virtuală.

Contribuţia programelor pentru furt şi fraudă în masa totală de atacuri malware este relativ mică – ajungînd la o cotă de 0,44% din toate atacurile din anul 2013, fiind cu 0,12% mai mult decît în anul anterior. Mai mult decît atît, în rîndul persoanelor expuse la atacurile malware de orice tip din anul trecut, 6,2% s-au confruntat cu cel puţin una din variantele de malware. Comparativ cu anul 2012, această cifră a crescut cu 1,3%.

"Kaspersky Lab" experts, malware authors are willing to pay tens of thousands for information about new vulnerabilities only for bypassing security programs and surpass the competition.

In 2013 "Kaspersky Lab" reflected the 28,4 million attacks using financial malware, which is 27,6% higher than a year earlier. The number of users attacked with similar malware also increased by 18,6%, to 3,8 million. In the study were used data on attacks with the help of Trojans bank, keyloggers, software for stealing Bitcoin virtual wallets and downloading programs for generating this virtual currency.

The contribution of theft and fraud programs in the total mass of malicious attacks is relatively small – they accounted 0.44% of all attacks in 2013, but it is at 0.12% more than a year before. Moreover, among people exposed to attacks by malicious software of all types in the past year 6.2% are faced with some 'financial' kind of malicious software. Compared with 2012, this figure increased by 1.3%.

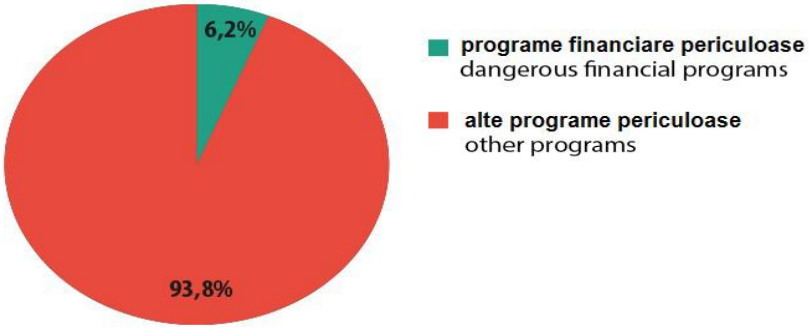

Fig. 2 .Utilizatorii atacaţi în anul 2013/
Fig. 2. Attacked users in 2013

În 2013, malware-urile financiare au afectat 6,2% din numărul de utilizatori din numărul total al persoanelor care au devenit obiective de malware.

Între numărul de atacuri şi numărul de utilizatori atacaţi s-a observat o corelaţie slabă. În 2012-2013, numărul lunar de atacuri varia cu zeci de procente. În primăvara anului 2012 acest număr a scăzut puternic şi a revenit la fostele lor poziţii abia în toamna anului 2013, dar numărul de utilizatori atacaţi nu a fost supusă brusc fluctuaţiilor şi aproape în fiecare lună arată o tendinţă pozitivă.

In 2013 malware financial specialization affected 6.2% of the number of users of all people who have become objectives of malware.

Between the number of attacks and the number of attacked users is noted a weak correlation. In 2012-2013 the monthly number of attacks varied by tens of percent. In the spring of 2013 it fell heavily and returned to their former positions in the autumn of 2013, but the number of users has not been exposed to such violent fluctuation and almost every month showed a positive trend.

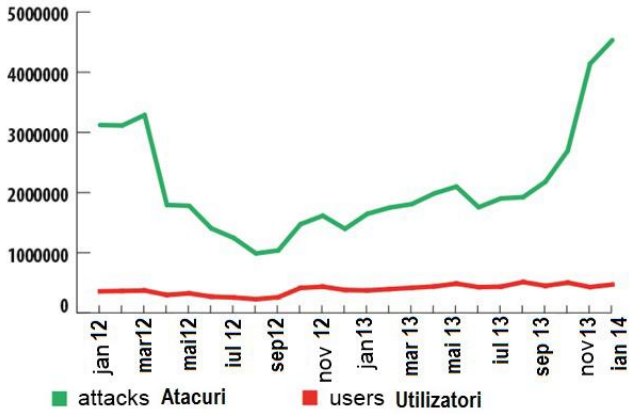

Fig. 3. Malware-ul financiar: atacurile şi utilizatorii atacaţi din anii 2012-2013/
Fig. 3. Financial malware: attack and attacked users in 2012-2013

Numărul de utilizatori atacaţi de malware-ul financiar a crescut pe parcursul anului 2013.

Reducerea numărului de atacuri în primăvara anului 2012 ar putea fi din cauza întreruperii activităţilor a mai multor grupuri de infractori cibernetici. La rândul său, creşterea bruscă a atacurilor în a doua jumătate a anului 2013 poate fi atribuită mai multor factori: atacatorii au găsit noi vulnerabilităţi periculoase în software-ul Oracle Java, care a făcut posibilă creşterea numărului de atacuri. De asemenea, în legătură cu rata de creştere valutară Bitcoin la sfârşitul anului, au fost introduse programe concepute pentru a fura portmoneele electronice cu acest Cryptocurrency.

Limitele ameninţărilor: atacul geografic şi utilizatorii atacaţi

Printre ţările cele mai expuse la atacuri de malware financiar în perioada 2012-2013, Rusia este lider, cu mai mult de 37% din atacuri. Ponderea oricărei altei ţari în cursul acestei perioade nu a depăşit pragul de zece la sută.

The number of attacked users by financial malware grew during 2013.

Reducing of attacks number in the spring of 2012 may be related to the termination of the activity of several groups of cyber criminals. In turn, the surge of attacks in the second half of 2013 can be attributed to several factors: the attackers found new dangerous vulnerabilities in Oracle Java software, which made it possible to increase the number of attacks. Also in connection with the Bitcoin growth rate at the end of the year were intensified programs designed to steal this electronic Cryptocurrency.

Border threats: geography attacks and attacked users

Among the most exposed countries of financial malware attacks in 2012-2013, Russia is the leader with more than 37% of attacks. The share of any other country during this period has not overcome even the 10% mark.

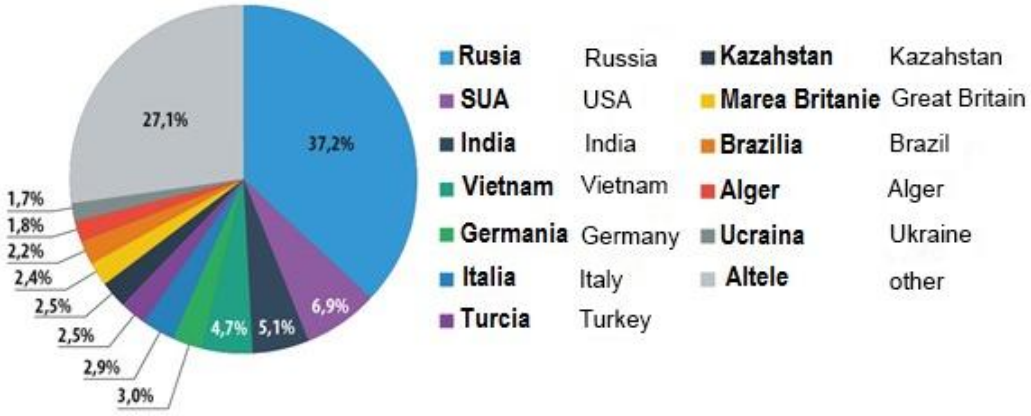

Fig. 4. Ţările cel mai frecvent atacate/
Fig. 4. The most frequently attacked countries

Topul celor 10 ţări au reprezentat aproximativ 70% din toate atacurile financiare pe parcursul a doi ani.

Rusia a devenit, de asemenea, un lider în creşterea de atacuri pe an. Cu toate acestea, numărul utilizatorilor atacaţi în ţară pe parcursul anului 2013 a scăzut uşor, în timp ce în majoritatea celorlalte ţări din *top zece* a existat o creştere.

On the top 10 countries accounted for about 70% of all financial attacks in two years.

Russia has also become a leader in the growth of attacks per year. However, the number of users attacked in in the country for 2013 slightly decreased, whereas in other countries in the top-ten there was an increase.

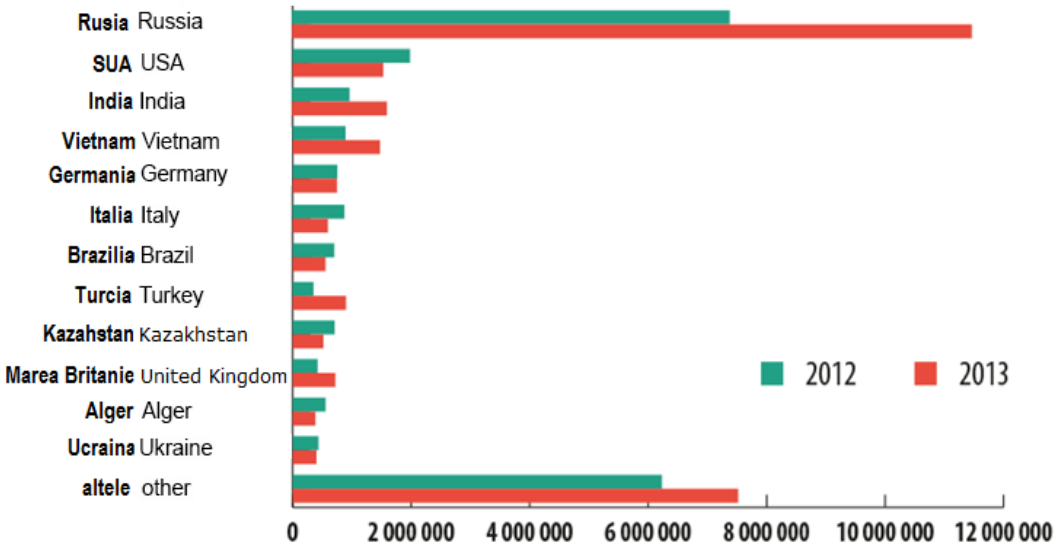

Fig. 5. Atacurile Geografice cu ajutorul Malware-ului financiar/
Fig. 5. Geography of financial Malware attacks

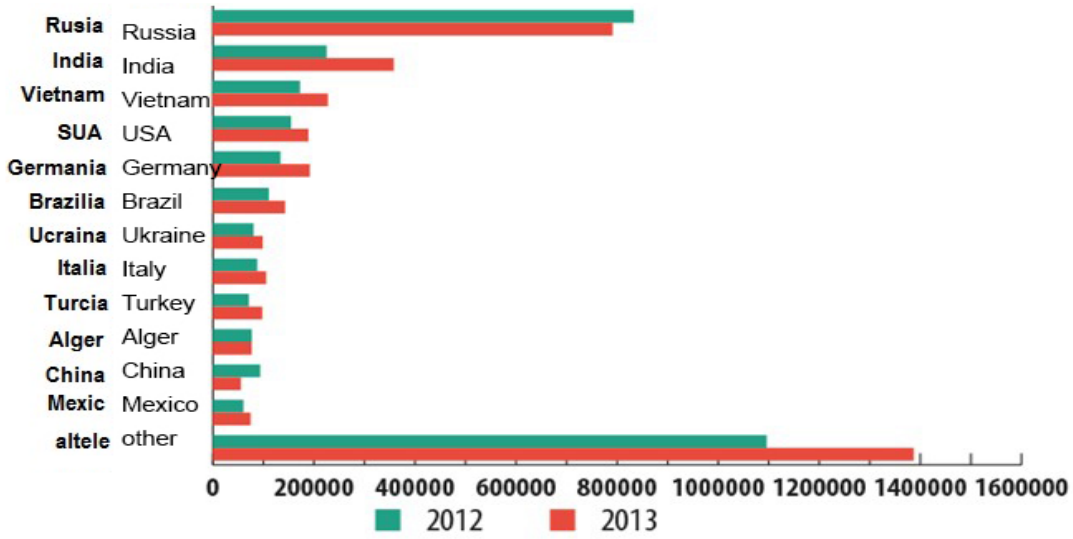

Fig. 6. Locaţiile atacate de Malware-ul financiar/
Fig. 6. The location of users attacked by a financial Malware

Numărul de utilizatori atacaţi de malware-ul financiar a crescut în opt din zece ţări – lider după numărul de atacuri financiare

Utilizatorii din Rusia riscă cel mai mult să devină victime ale atacurilor de malware financiar – în 2013 fiecare persoană luată în vizor de către infractorii cibernetici, a fost atacată în medie de 14,5 ori. În Statele Unite, această medie depăşeşte uşor cifra 8.

The number of users attacked by a financial malware increased for the year in eight of the top ten leaders countries.

Users from Russia were risked becoming a victim of financial attacks more often; in 2013 each person that was interested by financial cybercriminals was attacked with an average of nearly 14,5 times. Among the inhabitants of the United States this figure exceeded only 8.

Tabelul 1/Table 1

Numărul de atacuri prin intermediul soft-lor financiare periculoase /
The number of financial malicious attacks

Ţara / Country	Numărul de atacuri prin intermediul soft-lor financiare periculoase / The number of financial malicious attacks	Dinamica anuală / Annual Dymanics	Numărul de atacuri în mediu pe un utilizator / The number of attacks per user
Rusia / Russia	11 474 000+	55,28%	14,47
Turcia / Turkey	899 000+	156,41%	9,22
SUA/ USA	1 529 000+	-22,76%	8,08
Vietnam / Vietnam	1 473 000+	65,08%	6,43
Kazahstan/ Kazakhstan	517 000+	-26,88%	6,15
Italia / Italy	593 000+	-32,05%	5,61
India / India	1 600 000+	65,03%	4,47
Ucraina / Ukraine	401 000+	-7,54%	4,07
Germania / Germany	747 000+	-0,73%	3,9
Brazilia / Brazil	553 000+	-21,02%	3,87

Numărul mediu de atacuri/cetăţean, care a fost obiectiv al malware-ului financiar

Dintre ţările-lider în numărul de atacuri cibernetice, subspecii de ameninţări financiare online, sunt cele mai comune în Turcia şi Brazilia. Proporţia de utilizatori care au suferit atacuri financiare în aceste ţări s-a ridicat la 12% şi 10,5% din numărul total de utilizatori care s-au confruntat cu malware în 2013. În Rusia, cifra a fost puţin mai mult de 6%, în timp ce în SUA - doar fiecare al 30-lea atacat s-a confruntat cu una dintre amenintarile cibernetice financiare.

The average number of attacks, which accounted for everyone in the country, that has become the target of financial malware in 2013.

Among top cyberattacks countries, the financial subtype of online threats is the most common in Turkey and Brazil. The proportion of users who have suffered the financial attacks in these countries amounted to 12% and 10,5% of the total number of users faced with malware in 2013. In Russia this number was slightly more than 6%, while in the US only the 30th number of the attacked was faced with one or another financial cyberthreats.

Tabelul 2/ Table 2

Utilizatorii atacaţi de programele software financiar în 2013, şi cota lor in randul locuitorilor din ţările care se confruntă cu orice tip malware/
Financial software attack users in 2013 and their share among other residents of countries that faced any malware

Ţara / Country	Numărul de atacuri prin intermediul soft-lor financiare periculoase / The number of financial malicious attacks	Dinamica anuală / Annual Dymanics	Ponderea utilizatorilor, atacaţi de programe periculoase, % / The percentage of attacked users, %
Turcia / Turkey	97 000+	37,05%	12,01%
Brazilia/ Brazil	143,000+	29.28%	10,48%
Kazahstan / Kazakhstan	84 000+	5,11%	8,46%
Italia / Italy	105,000+	20.49%	8,39%
Vietnam / Vietnam	229 000+	31,77%	7,4%
India / India	358 000+	59,1%	6,79%
Rusia / Russia	792 000+	-4,99%	6,16%
Ucraina / Ukraine	98 000+	22,73%	6,08%
Germania / Germany	191 000+	43,22%	5,52%
SUA/ USA	189 000+	22,30%	3,1%

Dacă priveşti o hartă a lumii se observă, că ponderea atacurilor financiare este relativ scăzută în China, SUA, Canada şi multe ţări europene. Ţările-lider în acest sondaj sunt împrăştiate în întreaga lume, printre ţările ce au „întâietate" se numără Mongolia, Camerun, Turcia şi Republica Peru.

If you look at a world map, the share of financial attacks is relatively low in China, the US, Canada and many other European countries. The leader-countries are scattered around the world and they are Mongolia, Cameroon, Turkey and Peru.

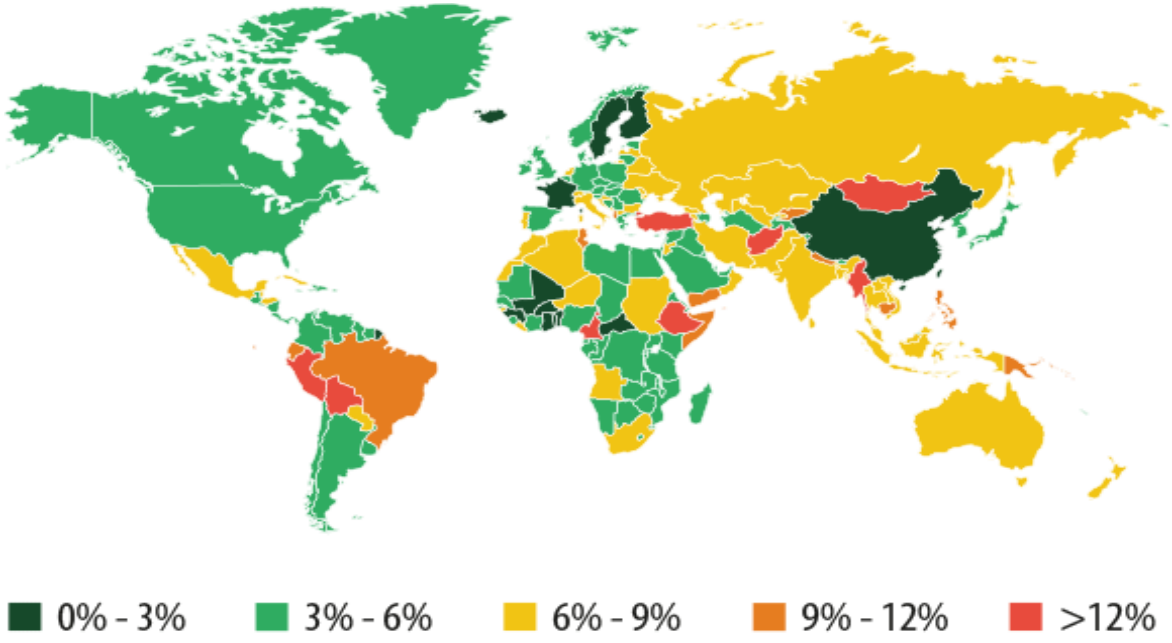

Fig. 7. Procentul de oameni ce se confruntă cu atacuri malware "financiare", într-un volum total de utilizatori atacaţi de orice tip malware/
Fig. 7. The percentage of users faced with "financial" malicious attacks in a total volume of users attacked by any malware

Cunoaşteţi duşmanul: tipurile de malware. Pentru a înţelege tipul de program malware, care vizează activele financiare ale utilizatorilor, în ultimul an s-a definit un grafic de ameninţări malware, experţii "Kaspersky Lab" divizînd instrumentele infractorilor cibernetici în categorii. Pentru scopurile acestui studiu au fost selectate mai mult de 30 de mostre de malware, cele mai notabile utilizate în atacuri. Proba a fost împărţită în patru grupuri, conform funcţiilor programelor şi obiectivelor lor: Bunker, keyloggers, instrumente pentru a fura portofele Bitcoin, şi programe de instalare ce generează însăşi Bitcoins. Cel mai mare grup este Bunker. Acest tip include

Know your enemy: the types of financial malware. In order to understand how malicious programs target financial assets, users defined the landscape of threats in the past year. The "Kaspersky Lab" experts shared tools of cybercriminals into categories. For the purpose of this study were selected more than 30 of the most notable malware samples used to financial attacks. The sample was divided into 4 groups depending on the functions of the programs and their objectives: the Bunkers, keyloggers, Bitcoin stealers and installers for generating Bitcoins. The Bunker is the largest group. This type includes Trojans and backdoors

troieni şi backdoors ce fură bani din conturi sau obține informațiile necesare pentru a fura. Printre alte tipuri de malware la fel de cunoscute sint Zbot, Carberp şi SpyEye.

for stealing money from the accounts or for stealing the needed information. Among other malware are known Zbo Carbert and SpyEye.

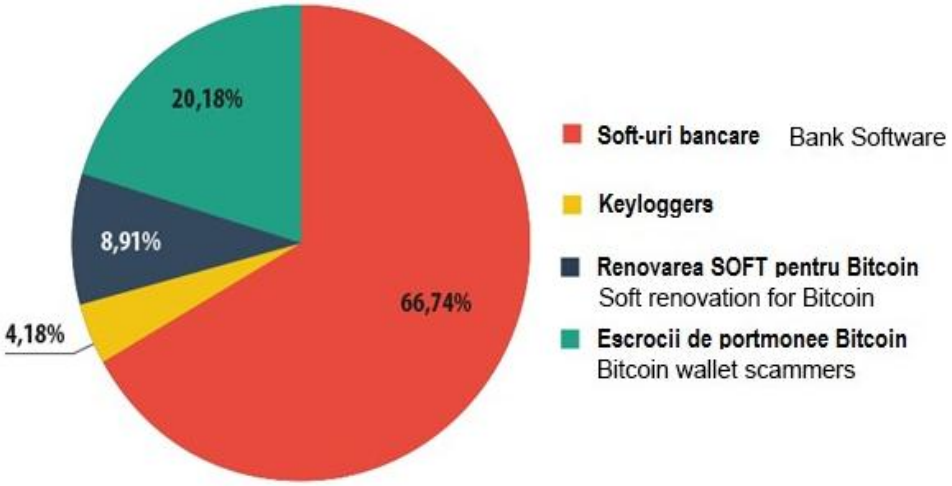

Fig. 8.Atacuri ce folosesc malware financiar în 2013/
Fig. 8. Financial malware attacks in 2013

Reprezentanții celei de-a doua categorii – keyloggers (keylogger) sînt proiectați în furtul informației confidențiale, inclusiv financiare. Troienii bancari oferă adesea funcții similare, de aceea popularitatea keyloggers ca un instrument independent este în declin. Cele mai populare dintre ele sunt Keylogger, Ardamax.

Celelalte două tipuri de malware rămase, asociate cu Cryptocurrency Bitcoin, au devenit în ultimii ani o pradă rîvnită de escrocii financiari. Acest software include instrumente pentru furtul portmoneelor Bitcoin şi instalarea ascunsă pe computerele ale aplicațiilor infectate pentru extragerea/expluatarea aceastei monede.

Primul tip este clasat ca malware ce fura fişierul-portmoneu, cu stocul de informații despre utilizatorul ce deține Bitcoins. Al doilea tip este clasificat ca ceva mai complicat: pentru instalarea de aplicații ce generează Bitcoins (mineritul), poate fi utilizat aproape orice model de malware cu capacitatea de a porni programele unui computer fără ştirea utilizatorului. De aceea, pentru acest stiudiu au fost selectate doar acele programe malware, care au fost observate în mod repetat în descărcarea şi pornirea uneltelor „de minerit”.

Trebuie remarcat faptul că această divizare nu necesită o precizie absolută. De exemplu, acelaşi keylogger poate fi folosit pentru a obține informații financiare şi pentru a fura conturile jocurilor online. Cu toate acestea, malware-ul este „specializat”, adică defineşte tipul predominant de infracțiuni comise cu ajutorul lor şi permite combinarea cu un anumit tip de criminalitate informatică – în acest caz cel financiar.

Rezultatul malware-urilor financiare

Printre riscurile financiare, în 2013 a jucat un rol de lider Bunker – malware-ul ce fura bani de la conturile utilizatorilor. Pentru anul curent, acestea au reprezentat aproape 19 milioane de atacuri cibernetice, care a reprezentat două treimi din toate atacurile financiare cu utilizarea malware-urilor.

The representatives of the second category, keyloggers are designed to steal confidential information, including financial. Bank Trojans often provide similar functions and the popularity of keyloggers as a standalone tool is on the wane. The most popular among them are KeyLogger and Ardamax.

The two remaining types of malicious software are associated with Cryptocurrency Bitcoin, which has become the coveted prey to financial scams in the last couple of years. This software includes tools for stealing Bitcoin-wallets and hidden installation on infected computers of applications for mining this currency.

The first type is ranked as malware for stealing the wallet-file, which stores information about the user that owns Bitcoins. The second type is somewhat more complicated to classify: for installing applications to generate Bitcoins (of mining) can be used in almost any pattern of malicious software, the ability to boot a computer without the user's knowledge. Therefore, only those samples of malware was selected to study that were repeatedly seen in the hidden downloading and running tools for mining.

It should be noted that this division does not require absolute precision. For example, the same keystroke logger can be used to obtain financial information and for stealing online games accounts. However, malware usually still have some 'specialization', which defines the predominant type of offences committed with their help that allows you lo link these programs with a particular type of cybercrime, in this case the financial one.

Banking malware comes

The bunkers is a malware for stealing money from the user accounts. For the year, it accounted for nearly 19 million cyber attacks, which amounted to two-thirds of all malicious software financial attacks.

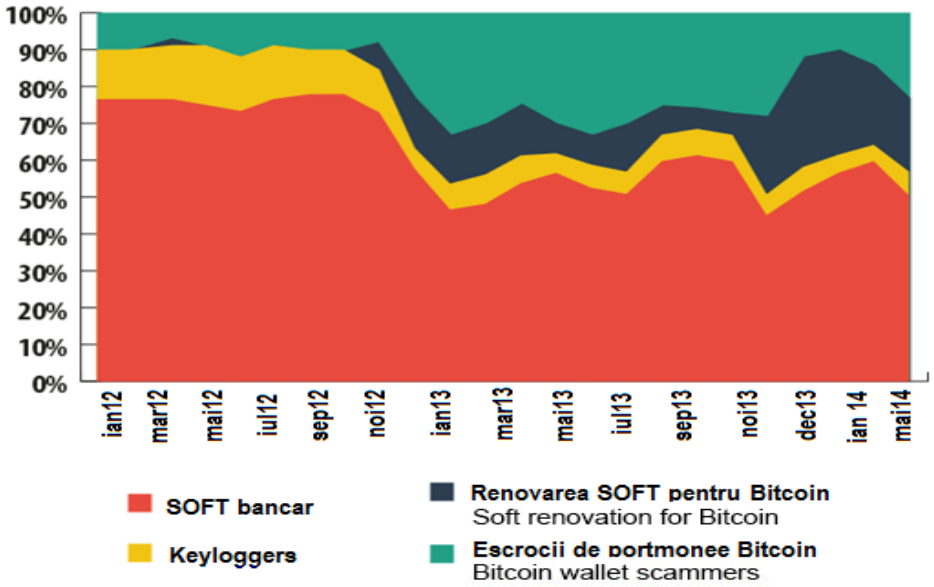

Fig. 9. Până la sfârşitul anului 2013, numărul total al utilizatorilor atacaţi lunar de programele ce fură Bitcoins şi a celor care descarcă şi mineresc Bitcoins a fost aproape de numărul Bunker/
Fig. 9. By the end of 2013, the total share of users attacked monthly by Bitcoins stealers and miners came close to the Bunker's

Cel mai activ dintre Bankeri, atât în numărul de atacuri cît şi în numărul de utilizatori a devenit programul troian Zbot (Zeus). Numărul de atacuri în urma modificarilor acestuia s-a mărit dublu pe parcursul anului, iar numărul de utilizatori atacaţi în ultimul an a depăşit topul celor zece bancheri la un loc.

The most active program has become Trojan Zbot (Zeus) both in the number of attacks and the number of attacked users. The number of attacks from its modifications increased more than doubled during the year. The number of users attacked in the past year increased other top bunkers indicators.

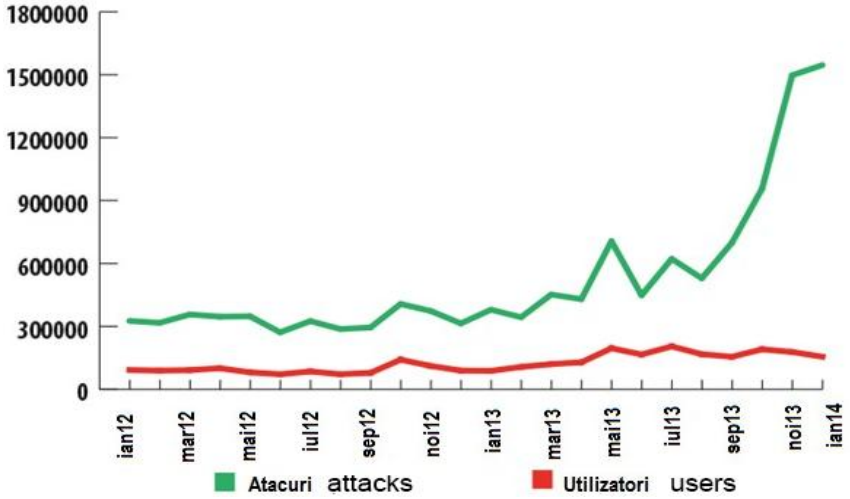

Fig. 9. Zbot, în anii 2012-2013/
Fig. 9. Zbot, 2012-2013

În 2011, codul sursă Zbot a fost accesat public, şi în baza lui au fost create şi continuă să fie create noi variante de malware care influienţează statistica atacurilor. Zbot este, deasemenea, cunoscut pentru faptul că pe baza sa a fost dezvoltată platforma Citadel – una dintre încercările de a transfera principiile de software comercial în crearea de malware. Utilizatorii Citadel nu doar că au cumpărat un troian, dar de asemenea, au obţinut un suport tehnic şi actualizări operaţionale care împiedică detectarea soluţiilor software anti-virus. De asemenea, în sursele Web a fost organizat un chat al hackerilor care pot posta cereri pentru introducerea de noi funcţii. La începutul lunii iunie 2013, Microsoft în colaborare

In 2011 the Zbot source code was in public access and on this basis have been created and continues to create new variants of malicious software that affects the statistics of attacks. Zbot is also known for the fact that it was the base of Citadel platform – one of the attempts to transfer the principles of commercial software in the creation of malware. Citadel users can buy a Trojan, but also get technical support and operational update that prevents detection by antivirus software. On Citadel Web Resources was organized hacker's forum, where they can post requests for the introduction of the new functions. In early June 2013, Microsoft in conjunction with the FBI announced the

cu FBI a anunțat închiderea mai multor rețele mari de Internet-bot care au făcut parte din Citadel, reprezentînd o mare victorie în lupta împotriva criminalității informatice. Cu toate acestea, după cum se poate observa din statisticile "Kaspersky Lab", acest eveniment nu a prea afectat răspândirea de malware, care vizează furtul de date financiare.

Scăderea puternică a numărului de atacuri troian Qhost se poate asocia cu arestarea creatorilor săi, care în 2011 au furat de la clienții uneia dintre cele mai mari bănci din Rusia circa 400 mii dolari. Autorii acestui malware au fost condamnați încă în 2012, dar acest lucru nu a împiedicat răspândirea în continuare a amenințărilor. Simplitatea relativă a instalării şi utilizării acestui malware atrage noi infractori.

closure of several large botnets that were part of Citadel, which was a great victory in the fight against cybercrime. However, as can be seen from the statistics of "Kaspersky Lab", this event is not affected too much the spread of malware for stealing financial data.

The strong decline on the number of Trojan Qhost attacks may be associated with the arrest of its creators, who stolt about $400 thousand from customers of one of the largest bank in Russia in 2011. The malware authors have been convicted again in 2012, but this did not prevent the further spread of the threat. The relative simplicity of setup and use of this malware attract more new intruders.

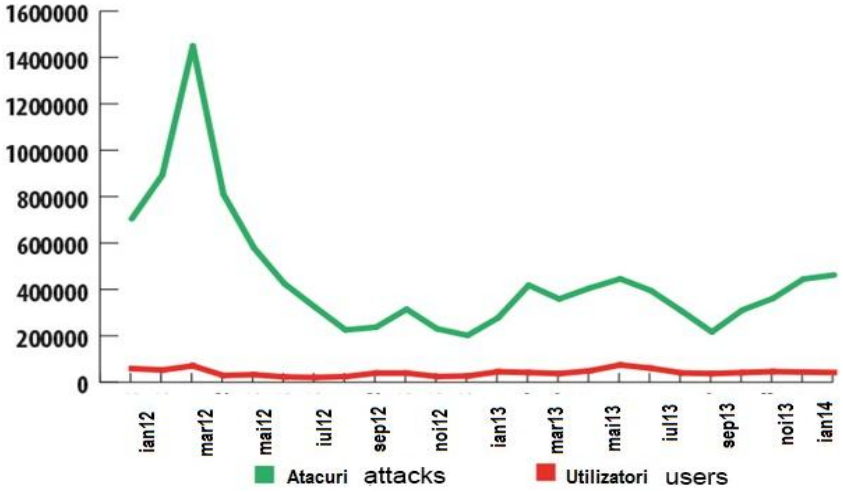

Fig. 10. Qhost, în anii 2012-2013/
Fig. 10. Qhost 2012-2013

Numărul de atacatori a troianului Carberp a scăzut în prima jumătate a anului 2013, după ce în primăvară a fost arestat creatorul troienilor, printre care se presupune că era şi creatorul acestui troian. Cu toate acestea, o creştere semnificativă a început în vara acestui an, ceea ce a permis ca în ultimele 12 luni să se revină la cifrele înregistrate în 2012. Acest lucru a fost în legătură cu publicarea codului sursă a malware-ului, devenind un impuls pentru crearea de noi versiuni ale troianului. Cu toate acestea, numărul utilizatori lor atacați de programele modificate ale acestui malware, a scăzut de mai multe ori pe parcursul unui an.

The number of Trojan Carberp attacks has fallen in the first half of 2013 after the arrest of Trojans users, among which, presumably, were the creators. However, a significant increase began in the summer, which allowed Carberp to catch up with the indicators of 2012. This is caused of malware source code publication in the public domain, which was the incitement to create new Trojan versions. Yet the attacked users number of this malicious software fell during the year several times.

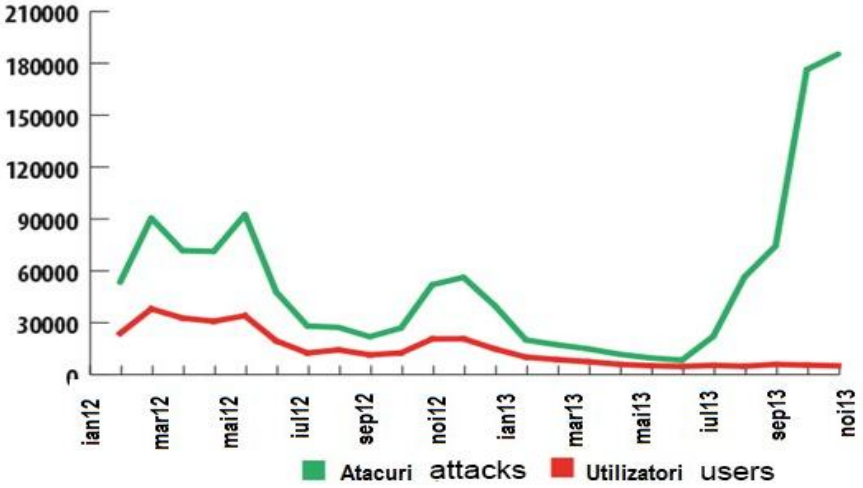

Fig. 11. Carberp, 20122013/
Fig. 11. Carpelp 2012-2013

Tendința generală este clară: după „liniștea” relativă din a doua jumătate a a. 2012, în 2013 infractorii, care își planificau atacuri cu ajutorul malware financiare, s-a intensificat, după cum reiese din creșterea numărului de atacuri și de utilizatori atacați.

The general trend is clear: after a relative ‘calm’ period in the second half of 2012, in 2013 the frauders intensified, as evidenced by the increase in the number of attacks and attacked users.

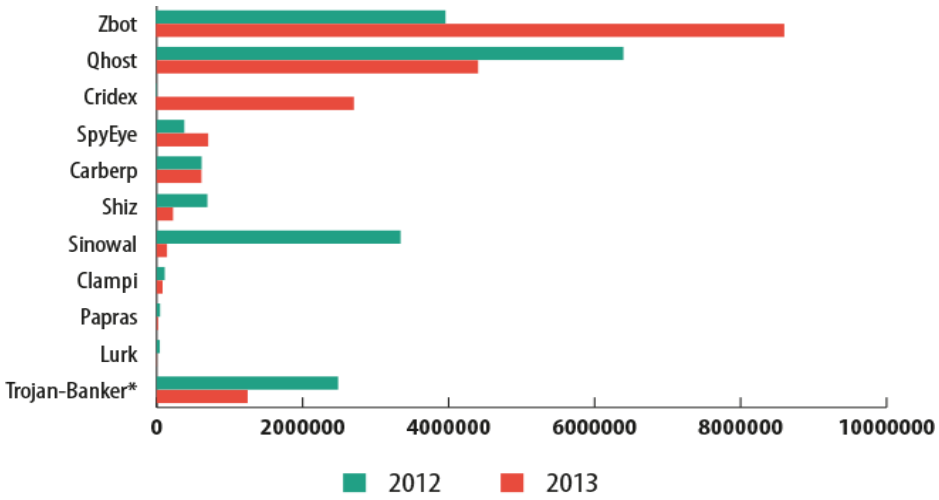

Fig. 12. Numărul de atacuri Bunker, în anii 2012-2013/
Fig. 12. The number of Bunker attacks in 2012-2013

** Trojan-Banker - înregistrare universală în bazele de date "Kaspersky Lab", care utilizează euristica pentru a detecta malware financiar/*
**Trojan-Banker is a universal record in “Kaspersky-Lab” databases, which uses heuristics to detect financial malware.*

Bitcoin: bani în vânt?

Bitcoin – valută electronică Cryptocurrency, care funcționează fără nici o reglementare de stat, deoarece este folosită de către oameni. Rețeaua distributivă, care asigură funcționarea aceste monede, a fost lansată în 2009. Inițial, moneda a fost utilizată de către persoane din sfera IT-industriei, treptat însă a devenit larg cunoscută. La popularitatea acestei valute, nu în ultimul rînd, a contribuit posibilitatea de a plăti pe unele dintre cele mai importante site-uri care vând bunuri ilegale. Utilizatorii aleg Bitcoin, grație anonimatului pe care această monedă îl oferă.

Bitcoin: money down the drain?

Bitcoin is an electronic Cryptocurrency that operates without any state regulation because of using it to people. Distributive network that provides Bitcoin was launched in 2009. Initially, the currency was used by people closed to the IT-industry, but gradually it became widely known. The chance to pay on some of the major sites that sell illegal goods contributed to the popularization of this currency. The users choose Bitcoin because of the anonymity that it provides.

Fig. 13. Reprezentarea Opțiunii Bitcoin pe hârtie/
Fig. 13. The representation of Bitcoin on paper

În teorie, pentru oricine poate primi Bitcoin, folosind puterea de procesare a computerului – acest proces se numeste minerit. Esența exploatării miniere – soluționarea seriilor de sarcini criptografice care sprijină funcționarea rețelei Bitcoin.

Mulți dintre așa-zișii bogătași-Bitcoin și-au câștigat averea

In theory, anyone can get a Bitcoin using the processing power of your computer and this process is called ‘mining’. The essence of mining is to solute series of cryptographic tasks that support the functioning of the Bitcoin network.

Many of Bitcoin-wealthy men earned their fortune

lor încă în faza incipientă a valutei, atunci când nu era percepută ca o lichiditate de fonduri. Cu toate acestea, după cum Cryptocurrency câştigă popularitate, pentru a obține Bitcoin din contribuția facilităților calculatoarelor devenea din ce în ce mai greu este una din caracteristicile sistemului, împreună cu un volum final de fonduri care vor fi puse în circulație. Până în prezent, complexitatea calculelor necesare a crescut în aşa măsură, încît mineritul de Bitcoin de pe computerele obişnuite a devenit nerentabil – profitul potențial este cu greu capabil să acopere costurile pentru electricitatea consumată.

while the beginning of this currency, when it was not perceived as a liquidity of funds. However, as Cryptocurrency gain popularity, to get a Bitcoin for the contribution of computer power becomes more and more difficult. It is one of the features of the system, along with a final volume of funds that will be released into circulation. To date, the complexity of the calculations required increased so much, that Bitcoin mining on conventional computers became unprofitable. The potential profit is hardly able to cover the cost of electricity.

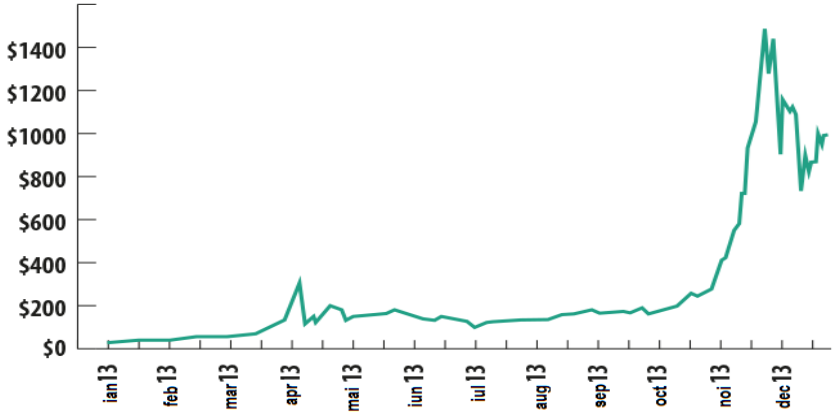

Fig. 14. Cursul Bitcoin la începutul anului 2013 a fost de circa 13,6 dolari, iar în decembrie, a atins un maxim istoric, de peste 1 200 de dolari/
Fig. 14. Bitcoin exchange rate in early 2013 was at around $13,6 and by December, when it reached the historic high, over $1.200

În decursul anului Bitcoin a crescut febril, trecând de 1.200 de dolari la sfârşitul lunii decembrie. Mai apoi cursul a mers în declin, ca urmare a poziției prudente a unor bănci centrale din mai multe țări în raport cu această moneda. Astfel, interdicția Băncii Populare Chineze de a mai lucra cu acest schimb valutar, schimbul de Bitcoin a scăzut, rata fiind de aproximativ o treime. În acelaşi timp, alte țări favorizau valuta Bitcoin – în special, Ministerul de Finanțe al Germaniei a recunoscut oficial acest tip de valută, iar în Canada şi Statele Unite ale Americii, chiar se instalau bancomate ce permiteau introducerea în numerar a Bitcoins.

Pe scurt, de la fenomenul Internet "de cameră", sprijinit de un mic grup de entuziaşti, Bitcoin a devenit în doar câțiva ani, dacă nu o monedă cu drepturi depline, apoi entitatea virtuală care reprezintă o valoare reală şi care se confruntă cu o cerere mare. Desigur, acest lucru nu a putut trece pe lîngă urechile răufăcătorilor. De cînd Bitcoin a început să fie vîndut pe bani reali în Internet, şi tot mai mulți comercianți au început a o foslosi ca mijloc de plată, prezintă tot mai mult interes pentru infractorii cibernetici.

Bitcoins sunt stocate pe computer într-un fişier-pungă special (wallet.dat sau altul, în funcție de aplicație). Dacă acest fişier nu este criptat şi un atacator ar fi capabil să-l fure, el poate transfera liber fondurile din contul tău în contul lui. Rețeaua Bitcoin permite oricărei părți accesul la istoricul tranzacțiilor realizate de oricare din utilizatorii ei. Adică poți urmări în care „portmoneu" au fost transferați banii furați. Dar din moment ce nimeni nu reglementează utilizarea monedei Bitcoin, nu poate respective să se plângă de furt nicăieri, ar fi un lucru inutil. Mai mult, pentru a fura Bitcoins, infractorii cibernetici pot folosi calculatoarele victimelor pentru mineritul "monedei" aproximativ la fel, precum

During the year Bitcoin grew feverishly and passed for $1.200 in late December. After this, exchange rate declined, including the position of the central bank wary of some countries towards this currency. Thus, the prohibition of the People's Bank of China served Bitcoin-exchange rate brought down by about a third. At the same time, Bitcoin is very favorable in other countries. In particular, the Ministry of Finance of Germany officially recognizes Cryptocurrency as a payment, and in Canada and the United States even are installed ATMs that allow to cash Bitroins.

In short, Bitcoin has become from the Internet phenomenon, supported by a small group of enthusiasts to the virtual entity that represents real value and experience high demand. Of course, this fact could not pass attackers' attention. Since Bitcoin was traded on exchanges online for real money, more and more vendors have started to accept the currency for payment, it became increasingly interest for cybercriminals.

Bitcoins are stored on your computer in special purse-file (wallet.dat or the other, depending on the application). If this file is not encrypted and is stealable, attackers can freely transfer funds from one account to their wallet. Bitcoin network allows to everyone to gain the access to the history of transactions made by any of its users. So, it is possible to identify to whose wallet were transferred the stolen money. But since no one can regulate Bitcoin, to complain about the theft elsewhere would be pointless.

In addition to stealing Bitcoins, cybercriminals can use the computers of their victims for mining coins, as sending

o faci pentru a trimite spam şi alte malware. Pe deasupra, există programe care solicită plată în Bitcoins pentru decriptarea datelor utilizatorului.

Graficul de mai jos arată dinamica atacurilor folosind instrumente-atacatori pentru a fura portofele-Bitcoin, precum şi malware "multifuncționale" observate în uneltele pentru minerit instalate. În plus, față de aceste detecții sunt afişate pe cererile de calculator unelte de minerit Bitcoin – ele pot fi instalate de către utilizator, sau pot fi aduse în calculator fără ştirea proprietarului. Produsele "Kaspersky Lab" includ cereri de minerit în categoria RiskTool. Acest lucru înseamnă că cererea conține funcții potențial-periculoase.

spam and other malicious activity. Additionally, there are programs that demand payment in Bitcoins for decrypting user data.

The following chart shows the dynamics of malicious tool attacks for stealing Bitcoin-wallets, as well as mining multifunctional malware. In addition to these, it indicates the case when detecting computer identify the applications for Bitcoin mining. It could be installed by the user or go to the computer without his knowledge. "Kaspersky Lab" products includes applications for mining in the RiskTool category. This means that the application contains a potentially dangerous functions.

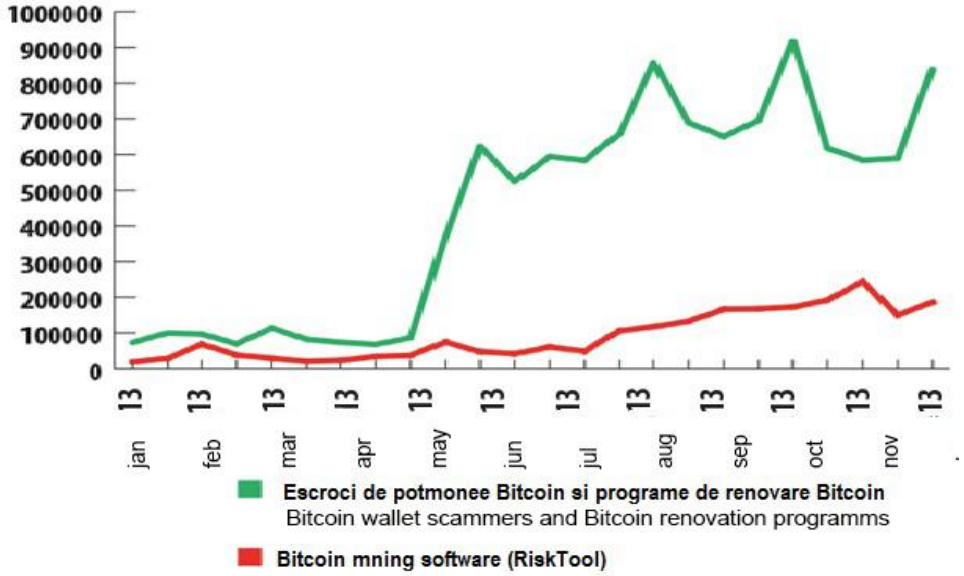

Fig. 15. Dinamica atacurilor
Fig. 15. Dynamics of malicious

După cum arată graficul, numărul de produse de protecție cu rezultate pozitive "Kaspersky Lab", cu privire la programele de răpire şi încărcările programelor de minerit Bitcoins, a inceput să crească în a II-a jum. a. 2012. O altă tendință interesantă aavut loc în 2013. De exemplu, unul dintre cele două produse de protecție importante pentru "Kaspersky Lab", de malware asociat cu Bitcoin, a fost în luna aprilie. Aproximativ în aceeaşi perioadă, rata de schimb Bitcoin a sarit la nivelul de mai mult de 230 dolari. Este evident că creşterea ratei de schimb ar putea provoca distribuirea mai activă de malware, pentru a fura sau mineri Bitcoins.

Cu toate acestea, în luna aprilie, prețul valutei a scăzut brusc la 83 de dolari. Recesiunea a fost urmată de recuperare a 149 dolari la sfârşitul lunii aprilie şi o stabilizare în luna mai. Din mai pînă în august Bitcoin „se plasa" la 90-100 de dolari, iar în luna august a început a creşte treptat. Acest proces este slab corelat cu situația de pe "frontul" malware deşi este posibil ca această stabilizare a Bitcoin să fi provocat un nou salt în luna august. Un alt salt brusc a numărului de atacuri a avut loc în luna decembrie. În această lună cursul Bitcoin a scăzut drastic - de la 1000 la 584 de dolari - apoi la fel de brusc a început să crească, ajungând la 804 de dolari la sfârşitul lunii. De asemenea, în luna aprilie este în creştere în mod constant numărul de produse de activare "Kaspersky Lab" software, pentru a genera Bitcoin. Această creştere a continuat până în octombrie, dar în noiembrie numărul alarmelor a început să scadă.

As the chart show, the number of positives protective products in "Kaspersky-Lab" began to grow in the second half of 2012.Another interesting trend was in 2013. For example, one of the two largest peaks of positive products in "Kaspersky Lab" was in April. Around the same time, Bitcoin exchange rate has jumped to the level of more than $230. It is obvious that the rate growth could provoke more active malware distribution, designed to steal or mining Bitcoin.

However, the currency price has fallen sharply to $83 in April. The recession was followed by recovery to $149 in late April and stabilization in May. From May to August Bitcoin held within 90-100 dollars, and in August became grow gradually. This process is weakly correlated with the malware situation, although it is possible that this stabilization of Bitcoin has provoked a new leap attacks in August. Another jump in the number of attacks occurred in December. Bitcoin rate first fell drastically (from $1.000 to $584), but then just began to grow and reached $804 at the end of the month.

Also in April the number of activation products in "Kaspersky Lab" increased steadily. This growth continued until October, but in November the number of alarms became to decline.

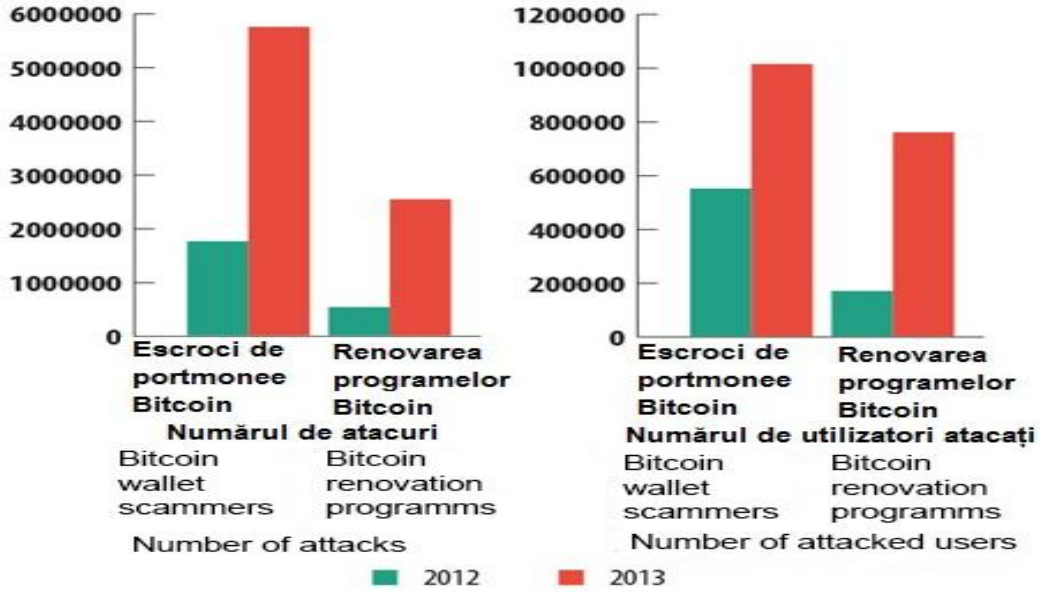

Fig. 16. Escrosi de portmonee, numărul de atacuri
Fig. 16. Bircoin wallet scammers, number of attascks

În general, în 2013 numărul de produse pozitive "Kaspersky Lab" şi numărul de utilizatori care se confruntau cu malware sau un potenţial dăunător asociat cu Bitcoin a crescut de mai multe ori comparativ cu anul 2012. De asemenea, este demn de remarcat că, începând din octombrie 2013 numărul de malware pozitive pentru, instalaţi software pentru minerit Bitcoin a început să scadă, iar numărul de operaţiuni ale hoţilor de „portofele", dimpotrivă – să crească. Acest lucru poate fi o consecinţă a caracteristicilor mai sus-menţionate ale monedei Bitcoin – cu cît mai multe monede se generează în sistem, este cu atât mai dificil de a crea altele noi. Acest lucru ar putea forţa atacatorii să se concentreze pe găsirea şi răpirea Bitcoin-portmoneelor deja cu valută generată.

Programele care vizează furtul de informaţii financiare este cu siguranţă un tip formidabil de malware de rea intenţie. Pericolul creşte, inclusiv, din cauza numărului foarte mare de potenţiale victime ale unor astfel de atacuri prin intermediul software-ului – practic fiecare proprietar al unui card de plastic, care navighează pe Internet cu calculatorul slab protejat, poate deveni victimă a răufăcătorilor. Cu toate acestea, calculatoarele şi laptop-urile nu sunt singurele dispozitive cu care utilizatorii se angajează în tranzacţii financiare. În zilele noastre, practic fiecare om modern are un smartphone şi/sau tabletă. În grupul de utilizatori ai serviciilor financiare aceste dispozitive sunt lacune suplimentare de care se pot folosi atacatorii.

Ameninţările „mobile" pentru online-Banking

Pentru o lungă perioadă de timp, dispozitivele mobile rămân a fi *Terra Incognita* pentru infractorii cibernetici. Acest lucru a fost posibil în mare măsură datorită gamei limitate de funcţii pentru primele generaţii de dispozitive mobile şi dificultăţile scrierii de software pentru ele. Dar, cu apariţia de smartphone-uri şi tablete multifuncţonale, cu conexiune la reţea, şi instrumentele publice disponibile pentru dezvoltarea de aplicaţii, totul sa schimbat. De mai mulţi ani, expertii "Kaspersky Lab" fixează creşterea anuală a numărului de programe malware care vizează dispozitive mobile, în special, care operează pe sistemul Android.

În 2013 Android a fost un obiectiv de prim-plan pentru atacurile malware. 98,1% din toate malware-urile mobile descoperite în 2013, urmăresc tocmai această platformă, indicând atît popularitatea sistemului de operare mobil, precum şi vulnerabilitatea arhitecturii sale.

Overall, the number of positives products in "Kaspersky-Lab" and the number of users faced with malicious or potentially malicious software associated with Bitcoin increased many times in 2013 compared with 2012. It is also noteworthy, that since about October 2013 the number of malware positives began to fall; but the number of operations on the kidnappers wallets on the contrary began to grow. This may be a consequence of the above features of Bitcoin currency – th more the system generates, the more difficult to create new ones. This could be force the attackers to focus in finding and kidnapping Bitcoin-purses with already generated Cryptocurrency.

Programs aimed at stealing financial information is certainly one of the most formidable type of malicious malware. The scale of the danger increases due to the huge number of potential victims of such software attacks. Practically every owner of a plastic card that goes to the Internet with poorly protected computers can fall for the bait intruders. However, computers and laptops are not the only devices with which users engage in financial transactions. Nowadays, almost every man have a smartphone and/or tablet. These devices are the additional loopholes in the pocket of users of financial services for attackers.

Mobile threats for online banking

For a long time, mobile devices remained Terra Incognita for cybercriminals. Due to the limited range of functions of the first generations of mobile devices and the difficulties with writing software for them. But everything changed with the appearance of smartphones and tablets. For several years, "Kaspersky-Lab" experts fixed the increasing in the number of malicious programs targeting mobile devices, in particular, the Android operating system.

In 2013 Android was a prime target for malicious attacks. 98,1% of all mobile malware discovered in 2013 was aimed precisely at this platform. Indicating, that both the popularity of the mobile operating system and the vulnerability of its structure.

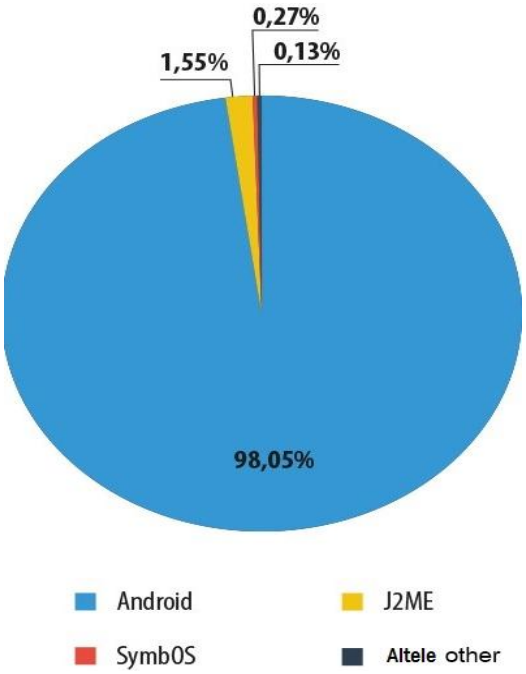

Fig. 17. Distribuția de malware mobil descoperit în 2013, pe platforme/
Fig. 17. Distribution of mobile malware discovered on the platforms in 2013

Majoritatea malware mobil are drept scop furtul de bani ai utilizatorilor. Straturile Trojan-SMS reprezintă uşile sparte şi alte malware-uri din categoria de stiluri Trojan. Cu toate acestea, creşterea numărului de programe concepute pentru a fura date de acces la sistemele bancare online şi a fondurilor a fost una dintre cele mai periculoase tendințe ale 2013 în domeniul malware mobil.

The majority of mobile malware aimed at stealing user's money. This ply Trojan-SMS, backdoors and other Trojan-style malware. However, the increase of the number of programs designed to steal data to access was one of the most dangerous trends of 2013 in the field on malware.

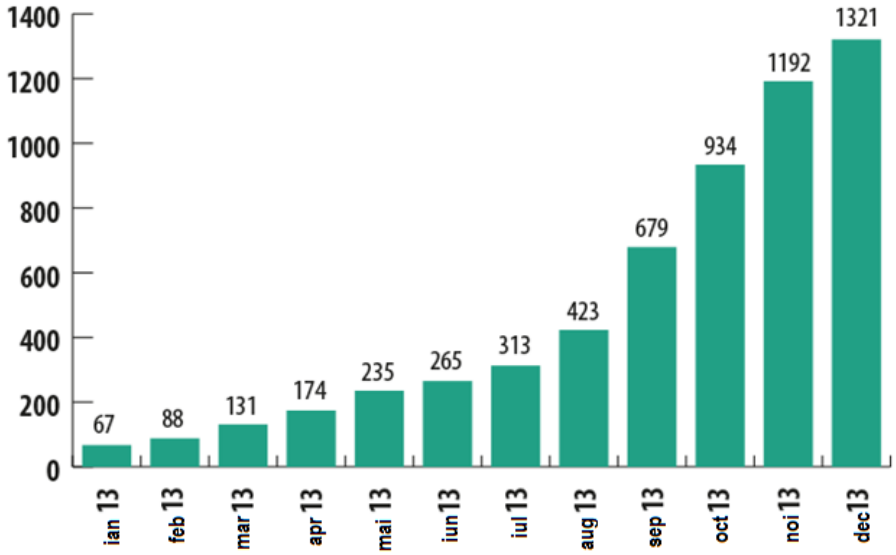

Fig. 18. Creşterea numărului de mostre de malware mobile bazate pe online banking, în colecția de "Kaspersky Lab" în 2013/
Fig. 18. The increase of the number of mobile malware based on online banking in the "Kaspersky-Lab" samples collection, 2013

Numărul de astfel de programe malware a crescut din iulie pînă în decembrie şi a ajuns să marcheze mai mult de 1300 de piese unice. În aproximativ acelaşi timp a început să crească şi numărul de atacuri blocate de produsele "Kaspersky Lab".

The number of such malicious programs actively grow from July to December and reached the mark of more than 1.3 thousand unique pieces. The number of attacks blocked by "Kaspersky-Lab" products began to grow at about this time.

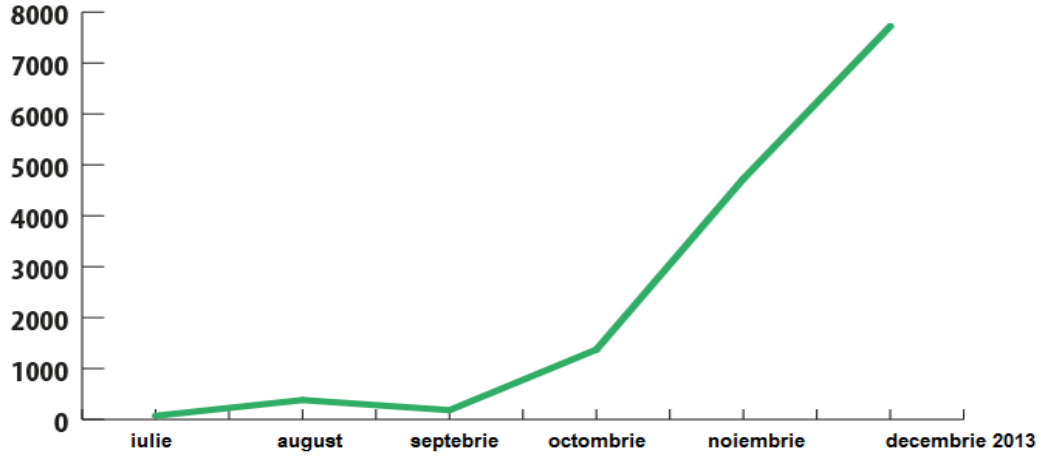

Fig. 19. Dinamica atacurilor cu utilizarea de malware-ului mobil, bazat pe online banking, în a doua jumătate a anului 2013/
Fig. 19. Mobile malware attacks dynamics, based on online banking in the second half of 2013

Malware-urile mobile care au ca obiectiv clienţii online banking se întâlneau şi anterior. De exemplu, ZitMo (celebrul "frate" mobil al lui Trojan Win32) a fost cunoscut încă din 2010, dar el nu a fost vazut în atacuri în masă, inclusiv din cauza funcţiulor sale specifice. ZitMo ar putea funcţiona doar în tandem cu ”desktop,, Zeus. Acesta interceptează login-ul şi parola pentru a accesa contul on-line a victimei, apoi funcţia principală a ZitMo este de a obţine parola unică pentru a confirma tranzacţiile în sistemul de online banking şi de a le transfera la atacator, care va folosi datele pentru a fura bani.

Un astfel de sistem de fraudă s-a întâlnit şi în 2013. De data aceasta, concurenţii principali ai lui Zeus au dobîndit noi programe malware (SpyEye, SpitMo, Carberp şi CitMo). Cu toate acestea, ele nu au fost observate în atacuri semnificative ca număr. Acest lucru poate fi corelat cu faptul că pe piaţa neagră cibernetică au apărut mai mulţi troieni "autonomi" capabili să funcţioneze fără un partener de pe "desktop".

Svpeng troian a devenit un exemplu de astfel de software, descoperit de experţii "Kaspersky Lab" în iulie 2013. Acest troian utilizează o caracteristică a unor sisteme ruseşti de mobile banking, prin care acesta este capabil să fure bani din contul bancar al victimei.

Mobile malware aimed at online customers are very well known. For example, ZitMo (famous Trojan Win32's brother) has been known since 2010, but it has not seen in mass attacks due to its specific functions. ZitMo could only work in tandem with the Zeus desktop. The latter intercepts the login and password to access the online account of the victim. Then ZitMo gets one-time password to confirm transactions in the system of online banking and transfer them to the attacker who used the data to steal money.

This fraud scheme was also in 2013. By this time, Zeus' major competitors acquired new malware programs (SpyEye, SpitMo, Carberp and CitMo). However, they have not seen in any meaningful amount of attacks. It can be connected with the fact that cyber block market get more anonymous Trojans, that are capable to operate without a desktop partner.

Trojan Svpeng is an example of such software. It was discovered by "Kaspersky-Lab" experts in July 2013. This Trojan uses a feature of some Russian mobile banking systems, through which it is able to steal money from the victim's bank account.

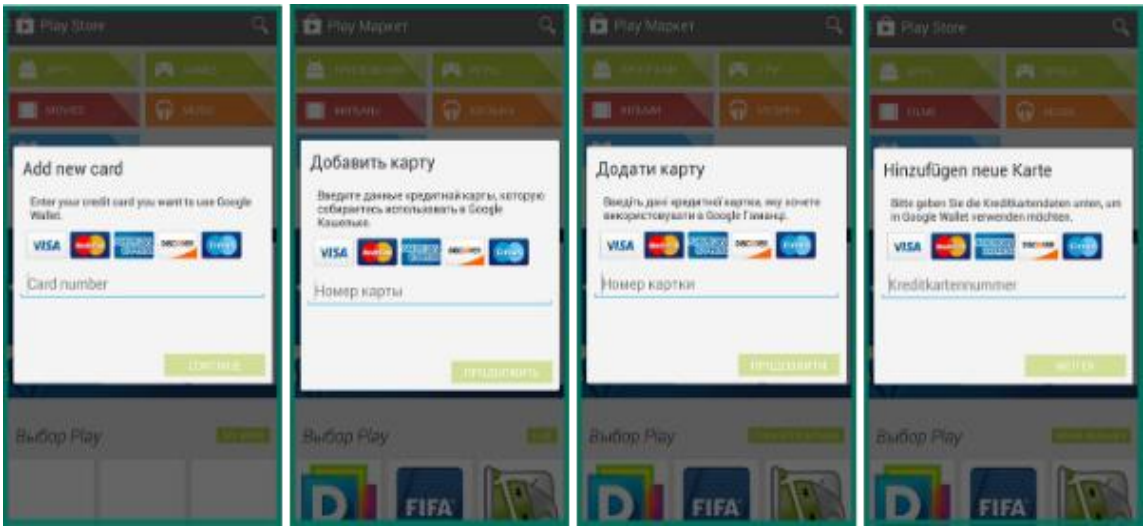

Fig. 20. Autentificare Fake interfaţă Svpeng/
Fig. 20. Fake login interface of Svpeng

În Rusia, unele bănci mari oferă clienților săi, cu reîncărcarea serviciilor de telefonie mobila, transfer de bani de pe un card bancar. Pentru aceasta clientul băncii trebuie doar să trimită un SMS cu un anumit conținut la un număr special al băncii. Svpeng trimite SMS-mesaj la serviciile de SMS-servicii a două astfel de bănci. În acest fel, proprietarul Svpeng poate ști dacă numărul smartphone-ului infectat arată prezența unui cont bancar. În cazul în care contul există, să obțină informații din bilanț. Mai apoi infractorul poate da comandă Svperg pentru a transfera bani din contul bancar al victimei la telefonia mobilă.

Pe viitor, furtul banilor de pe telefonia mobilă are o varietate de moduri, de exemplu, transferul într-un portmoneu electronic printr-un cont personal în cadrul operatorului de sistem sau trimiterea mesajelor banale la numere premium. În plus, Svpeng are funcțiile de a fura nume de utilizatori şi parole de acces la sistemele de online banking.

Încă cîteva exemple de troieni bancari periculoşi detectați de experții "Kaspersky Lab" – Perkele şi Wroba. Primul este un ZitMo analog, funcția sa principală fiind de a intercepta parolele o singură dată pentru a confirma tranzacții. Al doilea – caută pe dispozitivele mobile infectate aplicații pentru online banking, le şterge şi le înlocuieşte cu nişte copii false, cu ajutorul cărora colectează date de autentificare si trimite atacatori. Cele mai multe atacuri ale troienilor pentru banking mobile pe teritoriul Rusiei şi a țărilor vecine s-au înregistrat cu ajutorul "Kaspersky Lab" în 2013, Cu toate acestea, de exemplu, Perkele a atacat utilizatorii nu numai din Rusia, dar şi pe cei ai unor bănci europene. Wroba este focusat pe utilizatorii din Coreea de Sud.

Some Russian large banks provide to their customers the possibility to recharge their mobile phone money by transferring it from a bank card. To do this the bank customer have to send special SMS from their device to a special bank's number. Svpeng sends SMS-message to the SMS- services to two banks. In this way, the Svpeng owner could know whether the number is linked with a bank account. If it is, they may obtain the balance sheet information. Then attacker could give to Svpeng a command to transfer money from your bank account to the mobile.

In that follows, the attacker can steal money from the mobile account. For example, by a transfer through personal account in the operator system or just by sending messages to premium numbers. In addition, Svpeng has the functions of stealing usernames and passwords to online banking systems access.

Perkele and Wroba are more examples of dangerous banking Trojans detected by "Kaspersky-Lab" experts. The former is a ZitMo analog, its main function is to intercept one-time passwords for confirming transactions. The latter looks for the infected mobile device applications for online banking, it removes them and then loads fake copies with which collects authentication data and sends to the attacker.

Most of the mobile banking Trojans attacks were registered on the territory of Russia and neighboring countries by "Kaspersky-Lab" in 2013. However, for example, Perkele attacked not only Russian users, but also some European banks. Wroba focuses on South Korean users.

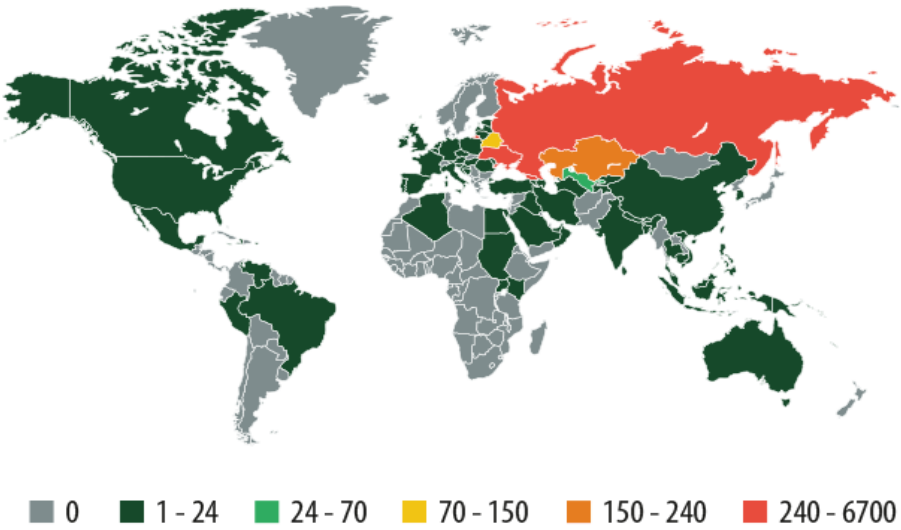

Fig. 21. Distribuția geografică a atentatelor cu malware Android-aplicații asupra băncilor în 2013/
Fig. 21. The geographical distribution of malicious banking Android application in 2013

În termeni absoluți, gradul de atac cu malware financiar al utilizatorilor de telefoane mobile produse de "Kaspersky Lab" este relativ mic. O tendință clară de creştere se poate urmări în următoarele şase luni. Ea semnalează că utilizatorii de telefonie mobilă, în special pe platformă Android, trebuie să fie foarte atenți cu privire la securitatea datelor financiare. Utilizatorii pe dispozitive iOS, de asemenea, să nu se relaxeze. Deşi programele malware concepute pentru a fura date confidențiale de la iPhone şi iPad nu se observă în sistemul de operare, se detectează în mod

In absolute terms, the extent of financial malware mobile attacks is relatively small. Obvious tendency can be seen for more than six months towards an increase in their number. It signals that the mobile users must be careful with their financial data, especially Android users.

The iOS users also should not relax. iOS regularly detects an error that allows to create such malware, although a lot of malicious programs are not observed in the operating system. An error detected by researchers at the

regulat erori, care permit de a crea astfel de malware. Una dintre cele mai proaspete exemple - eroarea detectată de cercetatori la sfârşitul lunii februarie 2014 şi care vă permite să definiți caracterele pe care utilizatorul le introduce de pe dispozitivul tastaturii virtuale. Folosind această vulnerabilitate, un atacator ar putea fura, inclusiv numele de utilizator şi parola pentru a accesa sistemul online banking.

Concluzie: Țineți evidența portofelului digital

Studiul arată clar că utilizatorii de monedă electronică sunt în pericol constant. Că lucrează utilizatorul cu contul prin internet banking, sau plăteşte pentru cumpărături în magazinul online – atacatorii, în aşteptare de bani uşori, îl privesc de peste tot.

În anul 2013 toate tipurile de riscuri financiare au arătat o creştere semnificativă. S-a dublat numărul de atacuri phishing cu utilizarea brand-urilor bancare. În timp ce numărul de atacuri financiare malware au crescut cu o treime.

Un segment de malware financiar nu a fost marcat de apariția unor "nou veniți", care ar putea pune în umbră slava lui Zbot şi Qhost. Aceştia şi alți troieni bine-cunoscuți sunt responsabili pentru cele mai multe dintre atacurile din ultimul an. Cu toate acestea, atacatorii au demonstrat încă o dată cât de sensibil reacționează la schimbările condițiilor de piață. Creşterea furtului de Bitcoin care a început la sfârşitul anului 2012, printr-o avalanşă de atacuri, a continuat şi în 2013.

Experți "Kaspersky Lab" dau urmatoarele sfaturi pentru a consolida protecția în fața amenințărilor cibernetice financiare:

Pentru afaceri

- Responsabilitatea pentru siguranța utilizatorilor revine, în mare măsură, businessului. Companiile financiare ar trebui să spună utilizatorilor despre amenințarea care o reprezintă ciberescrocii, şi să dea sfaturi cu privire la modul de a evita pierderile posibile din vina lor.
- Băncile şi sistemele de plăți trebuie să ofere clienților un sistem cuprinzător de protecție împotriva intruşilor. Un exemplu de soluționare este platforma „Kaspersky Fraud Prevention". Acesta oferă mai multe straturi de protecție împotriva fraudei.

Pentru utilizatorii casnici şi utilizatorii de servicii bancare online

- Autorii de malware adesea se bazează pe vulnerabilități în programele populare. Prin urmare, este necesar să se utilizeze numai versiunea nouă a aplicației şi instalarea imediată a actualizărilor de sistem de operare.
- Regulile universale de lucru în siguranță pe Internet ne ajută să reducem riscul atacurilor financiare. Utilizatorii ar trebui să aleagă parole puternice, care sunt unice pentru fiecare serviciu, să folosească cu grijă rețelele publice Wi-Fi, să refuze de a stoca informații confidențiale de către browser etc.
- Trebuie să utilizați produse fiabile pentru a vă proteja impotriva malware-ului, eficiența cărora este confirmată prin teste independente. În plus, unele produse de securitate, cum ar fi, Kaspersky Internet Security, au unelte built-in pentru operarea în siguranță a serviciilor financiare online.
- Dacă utilizați un smartphone sau tabletă pentru a accesa sistemul bancar online, sistemul de plată, sau a face achiziții de la magazine online, ar trebui să aveți grijă de

end of February 2014 allows to define the symbols that the user types. An attacker could steal login and password to access to the online banking system using this vulnerability.

Conclusion: Watch your digital wallet

The study clearly shows that users' e-money are in constant danger. Attackers lie in wait for money everywhere, even if the user works with his account via Internet banking or pays for purchases in the online shop.

All types of financial risks showed a significant increase in 2013. The number of bank phishing attacks has doubled. While the number of malicious malware financial attacks increased by a third.

Segment of the financial malware was not marked by the emergence of newcomers, that could outshine the glory of Zbot and Qhost. These and other well-known Trojans are responsible for most of the attacks in the past year. However, attackers have once again demonstrated how sensitive they react to changes in market conditions. The growth of stealing Bitcoin attacks had begun in late 2012 and continued in 2013.

"Kaspersky-Lab" experts give the following advice to strengthen the protection of the financial cyberthreats:

For Business

- The responsibility for the safety of users lies on business. Financial companies should tell to customers about the threat posed by cyberhawks and give advice on how to avoid losses due to their fault.
- Banks and payment systems must offer their customers a comprehensive system of protection against intruders. Kaspersky Fraud Prevention platform is an example of such solutions. It provides multiple layers of protection against fraud.

For home users and online banking users

- Malware writers often rely on vulnerabilities in popular programs. It is therefore necessary to use only the new versions of the application and immediately install operating system updates.
- Universal rules of online safety help reduce the financial attack risk. Users should choose strong passwords that are unique for each service, carefully use public Wi-Fi networks, refuse to store confidential information by the browser, and other.
- You should use reliable products against malware, which effectiveness is confirmed by independent testing. In addition, some security products, such as "Kaspersky Internet Security", habe build-in tools for safe operations of the financial online services.
- You should take care of the device protection with reliable solutions such as Kaspersky Internet Security for Android if you use smartphone or tablet to access the online banking system, payment system, or make purchases from online stores.

Conclusions

Many users are not familiar with the intricacies of such systems as Bitcoin and its analogues as Litecoin, Dogecoin and many others because of their youth. Therefore, "Kaspersky-Lab" experts prepared tips for safe use of Cryptocurrency:

- Stop using online services to store savings, instead use special wallets application.

dispozitivul de protecție cu soluții fiabile, cum ar fi Kaspersky Internet Security pentru Android, cu instrumente avansate pentru a proteja împotriva malware, phishing, precum și dispozitive pierdute sau furate.

Concluzii. Din cauza apariției recente ale Bitcoin şi analogilor săi, cum ar fi Litecoin, Dogecoin şi multe altele, mulți utilizatori nu sunt familiarizați cu complexitatea unor astfel de sisteme. Deaceea, experții Kaspersky Lab ne-au pregătit sfaturi pentru utilizarea în condiții de siguranță a banilor electronici:

- Nu utilizați servicii online pentru a stoca economiile, folosiți în schimb portofele speciale de aplicare;
- Împărțiți acumulările în mai multe portmonee – în caz de furt, va reduce pierderile la unul dintre ele.
- Aşezați portmoneele, folosite pentru instalațiile de depozitare pe termen lung, pe suporturi criptate. Ca alternativă, puteți utiliza portmoneele imprimate pe hârtie.

- Divide your savings in several purses. It will reduce losses in the case of theft from the one of them.
- Place used for long-term storage facilities purses on encrypted media. As an alternative, print your purses on paper.

Conclusions. Many users are not familiar with the intricacies of such systems as Bitcoin and its analogues as Litecoin, Dogecoin and many others because of their youth. Therefore, "Kaspersky-Lab" experts prepared tips for safe use of Cryptocurrency:

- Stop using online services to store savings, instead use special wallets application
- Divide your savings in several purses. It will reduce losses in the case of theft from the one of them.
- Place used for long-term storage facilities purses on encrypted media. As an alternative, print your purses on paper.

Referințe bibliografice / References

1. GRIBINCEA, A. *Relații economice internaționale: multimedia, cibermarketing şi internet*. Chişinău: ULIM, 1999. 82 p.
2. GRIBINCEA, A., OWEIDAH, J. Promoting factors in the educational reform in Israel. In: Studia securitatis. Sibiu, 2009, nr. 6, pp. 19-22.
3. GRIBINCEA, A., PERCINSCHI, N., CERNEI, M. Aspecte teorético-practice ale asigurării securității energetice prin intermediul utilizării inovațiilor în sectorul energetic. In: Sectorul serviciilor în sec. XXI: realizări, problema, perspective: simposion ştiințific internațional, 26-27 martie 2010. Chişinău: USM, 2010, pp. 221-226.
4. GRIBINCEA, A., STROE, C., EPURAŞ, O. Viitorul pieței carburanților. In: Problemele economice ale dezvoltării europene: conferința ştiințifică internațională, 25 martie 2011. Chişinău: ULIM, 2011, pp. 23-33.
5. Websense says educating employees will help stop phishing attacks. 2012, 9 october [accesat 5 ianuarie 2015]. Disponibil: http://www.cbronline.com/blogs/cbr-rolling-blog/websense-says-educating-employees-will-help-stop-phishing-attacks-091012
6. Как распознать фишинговые сообщения электронной почты или ссылки [accesat 5 ianuarie 2015]. Disponibil: http://www.microsoft.com/ru-ru/security/online-privacy/phishing-symptoms.aspx
7. Ваша информация в Интернете: о чем нам необходимо знать? [accesat 12 ianuarie 2015]. Disponibil: http://www.microsoft.com/ru-ru/security/online-privacy/information.aspx
8. OEM Spam Filtering Engines [accesat 5 ianuarie 2015]. Disponibil: http://www.solovatsoft.com/OEM_Spam_Filtering_Engines.html
9. How Can I Identify a Phishing Website or Email? [accesat 11 ianuarie 2015]. Disponibil: https://safety.yahoo.com/Security/PHISHING-SITE.html
10. Phishing [accesat 5 ianuarie 2015]. Disponibil: https://www.onguardonline.gov/phishing
11. Consumer AV/EPP Comparative Analysis - Phishing Protection [accesat 5 ianuarie 2015]. Disponibil: https://www.nsslabs.com/reports/consumer-avepp-comparative-analysis-phishing-protection-edition-1

Recomandat spre publicare: 12.01.2015