SECURIZAREA ELECTRONICĂ NAȚIONALĂ ŞI ESTIMAREA RISCURILOR ELECTRONICE ÎN SPAȚIUL ECONOMIC

Lect. sup. Elena BĂDĂRĂU, IRIM
Prof. univ. dr. hab. Alexandru GRIBINCEA, ULIM

Escrocii expediază e-mail-uri false sau creează Web site-uri false care mimează paginile de logare ale Yahoo! (sau paginile de logare ale altor companii de încredere, cum ar fi eBay sau PayPal), pentru a provoca utilizatorii să-şi dezvăluie numele şi parola. Această practică, adesea, este numită „phishing" („pescuit") – un joc de cuvinte, care ar însemna că escrocii pescuiesc datele personale ale conturilor utilizatorilor. Tipic, escrocii provoacă utilizatorii să introducă numele de utilizator şi parola pentru a obține acces la un cont online. Imediat ce au obținut accesul, ei pot folosi datele personale ale utilizatorului pentru a comite jaf de identitate, a schimba cardurile de credit, a goli conturile bancare, a citi poşta electronică şi a bloca accesul utilizatorilor la contul lor online prin schimbul parolei.

Dacă primiți un e-mail (sau mesaj instantaneu), care direcționează spre logare la un Web site, de la cineva necunoscut, atunci, fiți prudenți! Ați primit, probabil, un phishing e-mail cu link-uri la un phishing Web site. Un phishing Web site încearcă să fure parola contului dumneavoastră sau altă informație confidențială, făcându-vă să credeți că sunteți pe un Web site legitim. Dumneavoastră ați putea să ajungeți pe un asemenea site, când introduceți greşit un URL (adresă web).

Este, oare, legitim acest site? Nu vă lăsați convinşi de un site care arată ca şi real. Este uşor pentru hackeri să creeze site-uri, care arată identic cu cele originale, cu tot cu logo-uri şi altă grafică a Web site-urilor de încredere. Nota bene: dacă nu sunteți sigur de un Web site, nu vă logați. Cel mai sigur lucru pe care îl puteți face este să închideți şi să redeschideți browserul dumneavoastră şi apoi să introduceți URL-ul. Introducerea corectă a URL-ului este cea mai sigură metodă de a nu fi redirecționat la un site fraudulos.

Cuvinte-cheie: *e-comm, e-securitate, e-riscuri*
JEL: F2; F15

Introducere. Fraudele cibernetice, furtul de bani de pe conturile utilizatorilor online ai magazinelor, sistemelor de plăți şi ai sistemelor internet-banking, este practicat în primul an. Însă, mult timp, domeniul de activitate al infractorilor financiari a fost limitat de un şir de factori, în primul rând, răspândirea nu prea largă a mijloacelor electronice de plăți. Recentele alegeri în Parlamentul Republicii Moldova au demonstrat că diferite *cyber*-fraude pot deteriora activitatea multor

NATIONAL ELECTRONIC SECURITY AND ELECTRONIC RISKS ESTIMATES IN ECONOMIC SPHERE

Senior lecturer Elena BADARAU, IRIM
Professor Dr. Hab., Alexandru GRIBINCEA, ULIM

Fraudsters send fake emails or set up fake web sites that mimic Yahoo!'s sign-in pages (or the sign-in pages of other trusted companies, such as eBay or PayPal) to trick you into disclosing your user name and password. This practice is sometimes referred to as "phishing" — a play on the word "fishing" — because the fraudster is fishing for your private account information. Typically, fraudsters try to trick you into providing your user name and password so that they can gain access to an online account. Once they gain access, they can use your personal information to commit identity theft, charge your credit cards, empty your bank accounts, read your email, and lock you out of your online account by changing your password.

If you receive an email (or instant message) from someone you don't know directing you to sign in to a website, be careful! You may have received a phishing email with links to a phishing website. A phishing website (sometimes called a "spoofed" site) tries to steal your account password or other confidential information by tricking you into believing you're on a legitimate website. You could even land on a phishing site by mistyping a URL (web address).

Is that website legitimate? Don't be fooled by a site that looks real. It's easy for phishers to create websites that look like the genuine article, complete with the logo and other graphics of a trusted website. Important: If you're at all unsure about a website, do not sign in. The safest thing to do is to close and then reopen your browser, and then type the URL into your browser's URL bar. Typing the correct URL is the best way to be sure you're not redirected to a spoofed site.

Key words: *e-comm, e-security, e-risks*
JEL: F2, F15

Introduction. Cyber frauds, stealing money from the users' accounts of online-shops, Internet payment systems and banking systems are being practiced for years. However, the activity of financial scams has been limited for a long period of time by a number of factors, first of all by electronic means of payment, which are not very common. The recent elections in the Parliament of the Republic of Moldova have shown that *cyber* frauds can damage the activity of many structures. The methods are various. Antistructuri. Metodele sunt multiple. Software anti-phishing constă în programe de calculator care încearcă să identifice conținutul de *phishing* inclus în site-uri şi e-mailuri. Acesta este, adesea, integrat cu *browsere web* ca o bară de instrumente care afişează numele de domeniu real pentru site-ul şi clienții de e-mail care îl vizitează, în încercarea de a împiedica site-urile frauduloase de tipul deghizat să funcționeze ca şi alte site-uri legitime. Funcționalitatea anti-phishing poate fi inclusă ca o capacitate *built-in* de unele browsere web. Managerii utilizează parola pentru a facilita apărarea împotriva phishing-ului.

Banii electronici, în ultimii ani, devin tot mai importanți. Comoditatea de acces a sistemelor plăților electronice şi a serviciilor oferite prin intermediul serverelor online banking atrage atenția unui număr mare de consumatori, în plus, specialiştii în domeniul financiar şi băncile multor țări analizează posibilitatea de refuz total al banilor în numerar, în economiile naționale, în favoarea plăților fără numerar. Statistica obținută în baza datelor studiului global, realizat de agenția B2B International împreună cu „Laboratorul Kaspersky", în anul 2013, confirmă faptul creşterii popularității plăților digitale: 98% dintre respondenți au confirmat că utilizează regulat online banking-ul, sistemele de plăți şi comerțul electronic prin magazinele virtuale de pe internet.

Tendința de trecere la plățile fără numerar este însoțită de creşterea numărului de dispozitive, cu ajutorul cărora se efectuează tranzacțiile financiare. Conform aceluiaşi studiu, PC şi laptopurile rămân dispozitivele „majore", cu ajutorul cărora utilizatorii interacționează cu serviciile financiare – 87% dintre respondenți au confirmat că efectuează operațiuni cu bani electronici, folosind calculatorul staționar sau laptopul. Concomitent, ponderea dispozitivelor mobile, folosite în aceleaşi scopuri, atinge o cotă semnificativă: operațiile financiare efectuate de respondenți cu ajutorul tabletelor şi smartphone-urilor sunt de 22% şi 27%.

Aceste tendințe au atras atenția intruşilor. Creşterea rapidă a numărului de utilizatori în toate tipurile de sisteme electronice de plată atrage atenția infractorilor, care investesc tot mai multe resurse în scheme de escrocherie, realizarea cărora permite accesul, pentru început, la datele financiare şi mai apoi – la banii utilizatorilor. Deşi atacurile financiare constituie una dintre cele mai dificile şi cele mai costisitoare tipuri de punere în aplicare a atacurilor, ele sunt printre cele mai profitabile forme de criminalitate informatică, deoarece, în caz de succes, oferă acces direct la banii victimei. Tot ce rămâne de făcut este doar de a încasa banii, în timp ce, spre exemplu, autorul Software-ului virulent sau al spam-ului, sau proprietarul unei rețele botnet pentru DDoS-atacuri, încă mai trebuie să găsească cumpărători pentru serviciile lor.

„Laboratorul Kaspersky", de peste 16 ani se ocupă cu dezvoltarea mijloacelor de protejare împotriva tuturor tipurilor de atacuri cibernetice, inclusiv cele financiare.

phishing software consists of computer programs that attempt to identify *phishing* content that is contained on the sites and emails. It is often integrated with *web browsers* and email clients as a toolbar that displays the real domain name for visiting sites in an attempt to prevent fraudulent websites disguised as other legitimate sites. Anti-phishing functionality can be included as a *built-in* capacity of some web browsers. Managers use a password to help defending themselves against phishing.

For the last couple of years web money is becoming more significant. The convenience and ubiquitous availability of electronic payment systems and online banking services attract a great number of users and financial sphere regulators and banks of different countries are seriously considering the possibilities of total refusal of cash turnover of money in national economics in favour of non-cash calculations. The statistics got during a global survey, had been led by B2B International Agency together with "Kaspersky Laboratory" in 2013, which confirms the increasing popularity of digital payments: 98% of respondents said they regularly use online banking, payment systems or online shops.

The tendency of preferring non-cash payments goes with increasing of quantity of gadgets with the help of which financial transactions are being implemented. According to the data of the same research, PC and notebooks remain the "main" gadgets with the help of which users interact with financial services – 87% of the respondents said they accomplish operations with web money using desktop or portative computer. Nevertheless, the percentage of mobile gadgets, which are being used for the same purposes, is rather significant: respectively, financial operations implemented with the help of tablets and smartphones accomplish 22% and 27% of the interviewed ones.

All these tendencies have been noticed by malefactors. An impetuous increase of users of various electronic payment systems attracts lawbreakers and they invest more and more resources in fraudulent schemes the realization of which allows to get the access firstly for financial data and then to the very money of the users. Although financial attacks are the most sophisticated and expensive realizations of such attacks, they are also included in the list of the most profitable ways of cyber-crime, because, in case of success, they provide direct access to money of the victim. All we have to do is to take them out and cash the money meanwhile, for instance, the author of maleficent software or owner of bot network for DDos attacks or spam delivery needs yet to find customers for their services.

More than 16 years the "Kaspersky Laboratory" has practiced the development of security tools from various cyber-attacks, including financial ones. The development process of such technologies is

Procesul de dezvoltare a acestor tehnologii nu este posibil fără o analiză permanentă a noilor mostre ale Software-ului virulent, tehnicilor de inginerie socială şi ale altor instrumente pe larg folosite de infractorii care se ocupă de escrocherii financiare. Una dintre concluziile pe care le putem formula în baza acestei analize, constă în faptul că, spre deosebire de multe alte tipuri de atacuri, în atacurile virulente financiare, de regulă, se include un set de diferite mijloace: de la pagini de phishing, simulând paginile site-urilor instituțiilor financiare legale, până la folosirea vulnerabilă în Software a scrierii la comandă a programelor virulente.

Deoarece atacurile cibernetice financiare constituie un complex, analiza lor de influență, referitoare la nivelul de securitate al utilizatorilor site-ului, necesită o abordare complexă. Anume, de aceea, pentru pregătirea acestui raport, experții „Laboratorului Kaspersky" au analizat nu numai amenințările asupra platformei Windows, dar şi cele orientate spre platformele OS X şi Android; nu numai acțiunile răufăcătorilor specializați în PO, dar şi în alte programe care sunt potențial capabile să fure date financiare; nu răspânditele programe „troiene", dar şi atacurile phishing, care pot servi ca metodă eficientă pentru estorcarea datelor financiare importante. După părerea experților „Laboratorului Kaspersky", numai o asemenea metodă complexă ne permite atingerea scopului final: de a da un spectru maximal landşaftului „Cyber-pericolului" îndreptat spre finanțările online şi, în afară de aceasta, de a încerca să apreciem gradul de pericol prezentat de cyber-infractori.

Metodologia cercetării

În cadrul investigației, se folosesc date obținute de la utilizatorii răspânditei infrastructuri tenebre globale de către „Laboratorul Kaspersky", care s-a ocupat de prelucrarea datelor privind pericolul cu care s-au ciocnit utilizatorii produsului laboratorului sus-numit. „Kaspersky Security Network" a fost inițiat pentru ca extrem de repede să asigure utilizatorului produsele companiei şi informația despre cei mai noi viruşi. Datorită acestei rețele, timpul necesar pentru depistarea virusului şi „agățarea" link-ului despre virus din sistemul de operare se calculează în minute. O altă funcție a „Kaspersky Security Network" constă în prelucrarea statisticii despre viruşii care apar pe calculatorul utilizatorului, iar utilizatorii, la rândul lor, dau datele la „Kaspersky Security Network" benevol. Informația primită de la utilizatori respectivi a stat la baza acestei statistici.

La inițierea prezentei cercetări, s-a ținut cont şi de informația privind folosirea de către utilizatori a produselor „Laboratorului Kaspersky", care protejează de phishing platformele Microsoft Windows şi Apple (IOS x), de softul virulent (pe platformele Windows-ului) şi softul virulent mobil (pe platformele Google Android). În plus, în situația cu acele subsisteme de apărare elaborate de „Laboratorul Kaspersky", s-a luat în considerare şi statistica utilizatorilor atacați şi în raport, se analizează datele referitoare la geografia şi intensitatea atacurilor.

impossible without constant detailed analysis on new patterns of maleficent software, social engineering devices and other tools which are widely spread by malefactors who practice financial frauds. One of the most general conclusions that can be made according to this analysis is that in contradistinction to many other types of attacks, financial maleficent, as a rule, include an arsenal of many diversified means: from phishing web pages, imitating legal financial web pages, till applying vulnerabilities in popular software and ordered written maleficent programmes.

As financial cyber-attacks are complex, the analysis of their impact on the web users security level requires a complex treatment. That is why, while preparing this report, the experts of "Kaspersky Laboratory" considered not only Windows threats, but also threats aimed to platforms OS X and Android; not only specialized in PO maleficent software but also other programs which are potentially capable to reave financial data away; not only spreading of dangerous „trojan" programs, but also phishing attacks which might serve as an effective means of cajolery of valuable financial data. According to "Kaspersky Laboratory" only this complex way of treatment allows to reach the objective of this research, to give maximum large-scale picture of the „Cyber-attacks" landscape aimed to online finance and by the way, to try to evaluate the scale of danger carried by such cyber-attacks.

Research methodology

The present research contains data obtained from users of Kaspersky Security Network – apportioned global cloud infrastructure destined to handle operational data about threats with which "Kaspersky Laboratory" product users had faced. „Kaspersky Security Network" was created to inform users with information about the newest threats with maximum rapidity. Due to this web, a temporary interval between recently unknown threat detection and „adding" of signature for this threat in the base is calculated in minutes. Another function of „Kaspersky Security Network" is processing the depersonalized statistics about threats getting on users' computers. Users present data to „Kaspersky Security Network" voluntarily and this information is the basis of the present research.

In the framework of the research, there has been taken into account the information about "Kaspersky Laboratory" products, which protect from phishing on Microsoft Windows and Apple (IOS x) platforms, maleficent software (on Windows platform) and mobile maleficent software (on Google Android platform). Besides, in case of security subsystem products of "Kaspersky Laboratory", that show such a possibility, a statistics of attacked users was also considered. Furthermore, this report also includes analysis of data of geographical attacks and their intensity.

Cercetările cuprind anul 2013 şi, pentru comparare, se folosesc date colectate în anul 2012. În calitate de obiect al cercetării, au fost alese scopurile companiilor de phishing – numărul paginilor false blocate ale sistemelor de plată, ale sistemelor online Bancking, a internet- magazinelor şi ale altor interese financiare. Astfel, experţii „Laboratorului Kaspersky" au selectat câteva zeci de variante de softuri virulente, create special pentru sustragerea datelor financiare şi au analizat gradul lor de răspândire în ultima perioadă.

În anul 2013, *criptovaluta Bitcoin* a devenit foarte populară, de aceea, experţii „Laboratorului Kaspersky" au introdus-o într-o categorie aparte şi au analizat pericolele ce ţin de generarea şi sustragerea acestei valute, analizând evoluţia ei.

Cifre

Conform datelor obţinute de la sistemele de protecţie a produselor „Laboratorului Kaspersky", numărul atacurilor financiare, în 2012, s-a mărit esenţial.

Cifrele de bază obţinute în urma cercetărilor arată astfel:

- 31.45% din atacurile de phishing, în 2013, au fost săvârşite în sectorul financiar.
- 22.2% din atacuri au avut ca ţintă site-urile băncilor, rata phishing-ului bancar, comparativ cu anul 2012, s-a dublat.
- 59.5% din atacurile de tip phishing ale sistemului bancar au utilizat denumirile a doar 25 de bănci mondiale, celelalte atacuri s-au referit la mai bine de o mie de bănci.
- 38.92% din reacţiile sistemelor tehnologice de apărare a „Laboratorului Kaspersky" pentru calculatoarele Mac au revenit paginilor „financiare" phishing.

În continuare, vom cerceta detaliat dinamica atacurilor, geografia şi lista scopurilor acestora.

Pericole Phishing

Phishingul sau crearea copiilor false ale site-urilor, în scopul obţinerii datelor confidenţiale ale utilizatorului, constituie un pericol cibernetic destul de răspândit. Aceasta se explică prin faptul că, pentru desfăşurarea unei simple campanii phishing, infractorul cibernetic nu are nevoie de cunoştinţe aprofundate în domeniul programării, fiindu-i suficiente doar aptitudini de creare a unei pagini web. Scopul principal al phishing-ului este de a convinge jertfa că ea a intrat pe un site veritabil, şi nu pe unul fals. Deseori, asemenea încercări sunt încununate cu succes şi, de aceea, companiile phishing sunt folosite frecvent în calitate de instrumente de bază pentru obţinerea informaţiei necesare despre utilizator şi, ca parte componentă a unui atac complex, pentru atragerea utilizatorilor pe site-ul de pe care, pe calculatoarele lor, va fi instalat soft cu caracter virulent.

După cum denotă cercetările, paginile phishing, deseori, se utilizează în atacurile „cyber", îndreptate spre furtul datelor financiare ale utilizatorilor. Dar, până a începe o analiză desfăşurată a acestor atacuri, va fi

The research covers the data collected during 2013, but also those of 2012 for comparison. As the subject of the research were chosen targets of phishing companies – number of blocked downloads of phishing, payment systems pages, online Banking systems, online – shops and other financial purposes. Moreover, "Kaspersky Laboratory" experts have selected a few dozens of maleficent software, specially created for stealing financial data and analysed their prevalence extent during period of the research.

In 2013, *Bitcoin crypto currency* has become extremely popular, "Kaspersky Laboratory" experts selected in a separate category those threats which are connected with generation and stealing of this currency and tracked its evolution.

Numbers

According to the data got from security subsystems of "Kaspersky Laboratory", in 2012, the number of financially-oriented attacks had considerably increased.

The main numbers got during research are as follows:

- 31,45% of all phishing attacks in 2013 were financially oriented.
- 22,2% of attacks were as for fake bank sites; in comparison with 2012 the percentage of bank phishing doubled.
- 59,5% of bank phishing attacks exploited denominations of 25 international banks, the other attacks were as for more than one thousand other banks.
- 38,92% of all security technology activations of "Kaspersky Laboratory" on Mac computers were „financially" oriented phishing pages.

Further in this research we will consider dynamics of attack in details and also their geography and objectives list.

Phishing threats

Phishing or creation of false copies of sites with purpose to get confidential data of users is a very wide spread cyber threat. In a lot of aspects it is connected with the fact that development of an ordinary phishing company a cyber-criminal needn't be master of programming, the skills of creating web-sites is enough. The main objective of phishing is to persuade the victim that she/he entered the real site, not fake one. Frequently such attempts turn out to be successful because phishing companies are often used as the main tool for getting important information about users and as a part of a complex attack- for attracting users on the site from which the deleterious software will be installed on their gadgets.

As a result of our investigation phishing sites are oftentimes used in „cyber", attacks directed to stealing financial dada of users. But before proceeding to detailed analysis of these attacks it would be useful utilă informaţia despre tabloul general al pericolelor phishing din anul 2013.

Atacurile şi utilizatorii

Produsele de apărare ale „Laboratorului Kaspersky" dispun de 4 subsisteme pentru apărarea de atacurile phishing. Bazele anti-phishing – similar bazelor signaturilor failurilor cu virus – se păstrează în calculatoarele utilizatorilor şi conţin o listă cu cele mai răspândite şi actuale, la momentul producerii, link-uri pe bază de phishing. Al doilea subsistem este o bază anti-phishing „nor" – la care se adresează produsele de apărare ale „Laboratorului Kaspersky" în cazul, când utilizatorul descoperă un link suspicios, despre care încă nu există informaţii în baza anti-phishing de securitate locală. Baza „nor" se reînnoieşte mai repede decât cele locale şi este prevăzută pentru depistarea celor mai noi phishing-atacuri.

În afară de aceasta, în produsele anti-phishing, lucrează două sisteme automate de depistare a link-urilor phishing şi a paginilor: poşta şi pagina web din sistemul poştal verifică link-urile şi mesajele din poşta electronică a clientului, dacă acesta lucrează cu programele Microsoft, Outlook. Sistemul web de depistare automată verifică tot ce apare în brauzerul utilizatorului, conducându-se de lista regulilor euristice şi este capabilă să depisteze noi pagini phishing, despre care nu există informaţii în nicio bază.

Pentru raportul dat, „Laboratorul Kaspersky" utilizează date selectate doar din sistemele web de protecţie, deoarece, ca regulă, ea reacţionează în cazul în care informaţia despre paginile noi phishing lipseşte în baza de date a „Laboratorului Kaspersky" şi, în afară de aceasta, în comparaţie cu bazele locale şi tenebre, ne permite să depistăm scopul atacului phishing. În plus, dacă bazele anti-phishing sunt capabile să descopere simplul atac phishing, prin link-ul în scrisoare ori în sistemul de căutare Google, atunci sistemul automat de depistare web reacţionează în momentul trecerii utilizatorului în link, adică din momentul când persoana, deja, parţial, este implicată în schema frauduloasă pregătită de răufăcători.

to demonstrate the whole picture of phishing threats in 2013.

Attacks and users

Security products "Kaspersky Laboratory" have 4 subsystems for protection from phishing attacks. Anti-phishing bases – are similar to signatures bases of deleterious files which are held on the users' gadgets and contain a list of most spread and actual phishing links produced for the given moment. The second subsystem is a „cloud" anti-phishing ases the security "Kaspersky Laboratory" products of which appeal in case if the user faced a suspicious link information about which is not found in the local anti-phishing base. The „cloud" system updates quicker than local ones and is intended to detect the newest phishing attacks.

Besides, there are two automatic systems detecting phishing links and pages in antivirus products: mail and web systems. The mail system checks links in messages of user's e-mail if he works with one of popular post clients on his computer Microsoft Outlook. The automatic system of web detecting checks everything that is in the user's browser, guided by a set of heuristic rules is capable to detect absolutely new phishing pages information about which can't be found in any base.

For this research "Kaspersky Laboratory" used data got only from system of web-detecting, because as a rule, it works out only in case if information about brand new phishing site is not found in "Kaspersky Laboratory", besides, unlike local and cloud bases it allows to determine the aim of phishing attack. Moreover, if anti-phishing bases are capable to determine a phishing attack just by having a link in the mail or search line of Google the detecting system automatically works in the moment of user's crossing the link, i.e. in the very moment when a person is partly involved in fraudulent scheme prepared by malefactors.

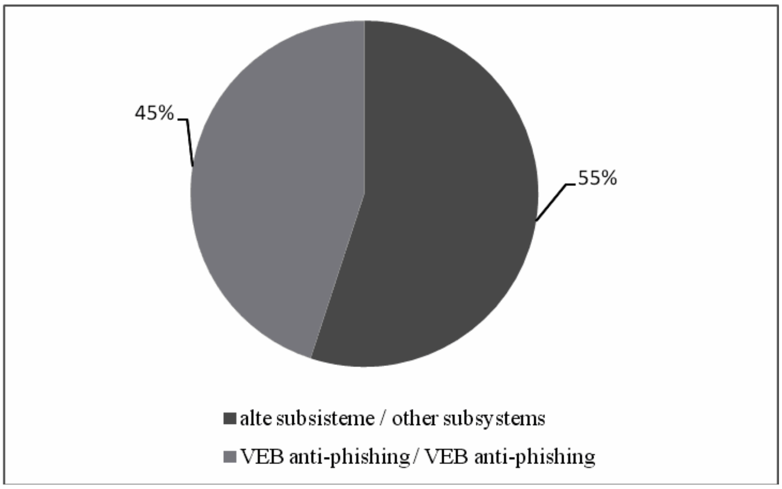


Figura 1. Ponderea atacurilor, blocate de programe anti-phishing în 2013 /
Figure 1. Share of attacks, phishing programs blocked in 2013

Conform datelor „Laboratorului Kaspersky” din anul 2013, circa 39,6 milioane de utilizatori au fost afectați de atacuri phishing. Comparativ cu anul 2012, cifra aceasta s-a majorat cu 2,32%.

În total, din toate subsistemele de apărare anti-phishing, în „Laboratorul Kaspersky”, au intrat mai mult de 600 de milioane de înștiințări de la utilizatorii care s-au confruntat cu atacuri de tip phishing, cu link-uri şi pagini web virulente. În anul 2012, cifra era aproximativ aceeaşi, cu toate acestea, numărul atacurilor anti-phishing euritstic, blocate de web, s-a mărit considerabil cu 22,2% – de la 270 de milioane până la circa 330 de milioane atacuri în 2013. Acest fapt este legat şi de îmbunătățirea sistemului de securitate.

Geografia atacurilor

În 2013, majoritatea atacurilor phishing blocate au parvenit din SUA – circa 30,8%, Rusia – 11,2%, Germania – 9,32% din totalul atacurilor.

According to data of “Kaspersky Laboratory” in the year 2013 about 39,6 million users faced phishing. In comparison with 2012, this number increased up to 2,32%.

There had come more than 600 million of notifications of users facing phishing links and pages from “Kaspersky Laboratory” anti-phishing system. In 2012 this number was mostly the same.. In the same period this quantity of attacks, blocked by heuristic anti-phishing significantly increased up to 22,2%, from 270 million in 2012 to 330 million in 2013. It is associated with constant improvement of heuristic detecting system.

Geography of attacks

In 2013 the majority of blocked phishing attacks were received in the USA – about 30.8%, Russia – 11.2%, Germany – 9.32% of all attacks.

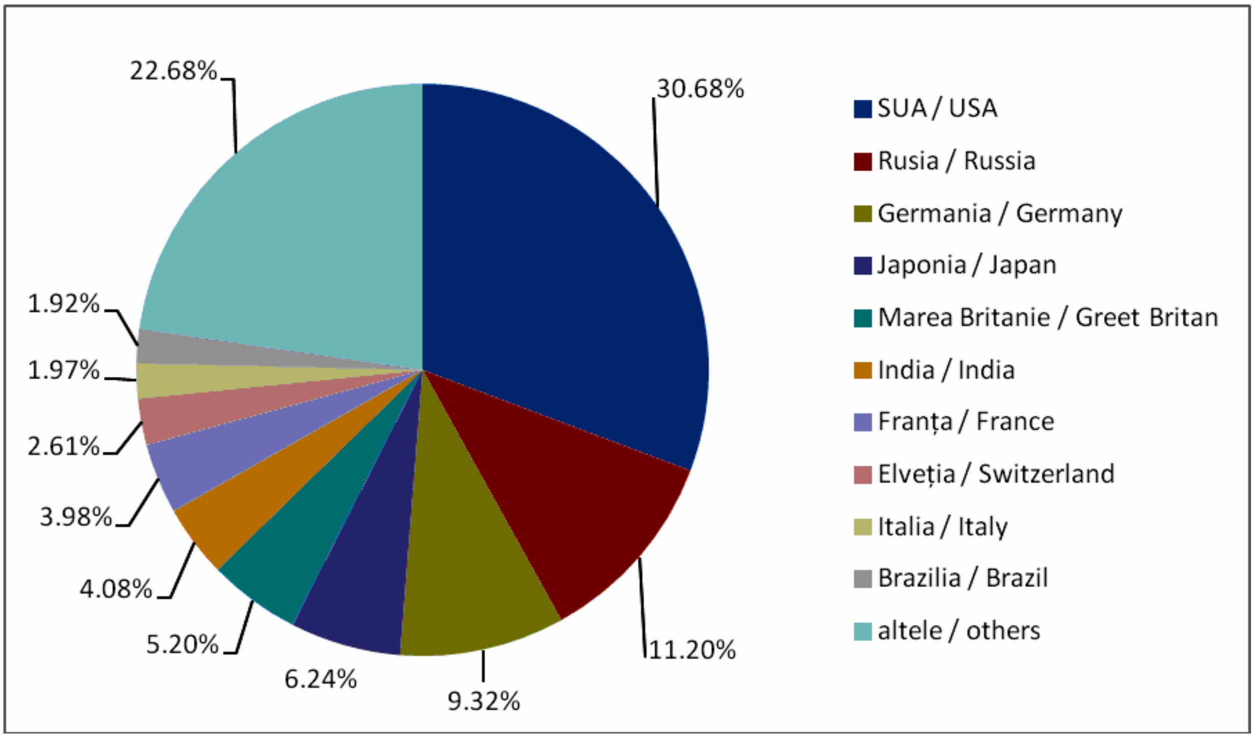


Figura 2. Țările care au fost supuse atacurilor în 2013 /
Figure 2. Countries where attacks were submitted in 2013

Din 2012, în topul celor mai des atacabile țări, au survenit schimbări considerabile. De exemplu: atacurile împotriva utilizatorilor din Rusia au scăzut cu 9,19%, iar atacurile împotriva utilizatorilor din SUA, dimpotrivă, s-au mărit de la 17,56% în 2012 până la 30.8% în 2013. De asemenea, s-a mărit numărul atacurilor şi asupra utilizatorilor din Germania de la 5,83% până la 9,32%.

Cauzele de împărțire geografică a acestor atacuri pot fi diferite. Astfel, în cercetările anterioare noi, ne-am ciocnit deja de micşorarea atacurilor în diferite țări şi

In comparison with 2012 the top of most frequently attacked countries had significant changes. For instance, a percentage of attacks against users from Russia decreased to 9,19 % and the percentage of attacks against users from USA, on the contrary, significantly increased from 17,56% in 2012 till 30,8% in 2013. Attacks against users from Germany also increased from 5,83 till 9,32%.

There can be plenty of reasons for such geographical allocation of attacks. In previous research mărirea lor în altele. Micşorarea numărului de atacuri poate fi influențată de asemenea factori, precum: înăsprirea măsurilor de luptă împotriva cyber-infracțiunilor şi complicarea procedurii de înregistrare a datelor personale etc. Creşterea poate fi cauzată de numărul de utilizatori obişnuiți să încarce rețele sociale pe internet şi pe web, în parte, pentru a vizita internet-magazine şi altele. Cu cât mai des utilizatorii din altă țară încarcă web pagini, cu atât mai des ei riscă să se confrunte cu pagini web false, adică cu pagini phishing.

Scopul

După cum se observă din diagrama de mai jos, majoritatea atacurilor au fost efectuate asupra rețelelor sociale – circa 35,4%. Ținte financiare au devenit adresele bancare – sistemelor de plăți din internet-magazine le reveneau 31,45% din atacuri. Pe locul trei, cu 23,3%, se situau adresele poştale.

we had already faced with decreasing of attacks in a range of countries and their increasing in other ones. For decreasing of number of attacks can influence such a factor as amplification of defending measures with hyper scrupulousness; complication of registration procedure of domain names etc. The increase of attacks can be provoked by natural increase of number of Internet users and separate web-resources, social networks, online shops and other. The more often users in a separately considered country load web-pages, the more risk they have to face phishing pages.

The Objective

As shown in the diagram below most attacks go back social networks - about 35.4%. Financial targets returned false bank addresses, Internet payment systems in stores were 31.45% of attacks. On the third place with 23,3% were e-mail addresses.

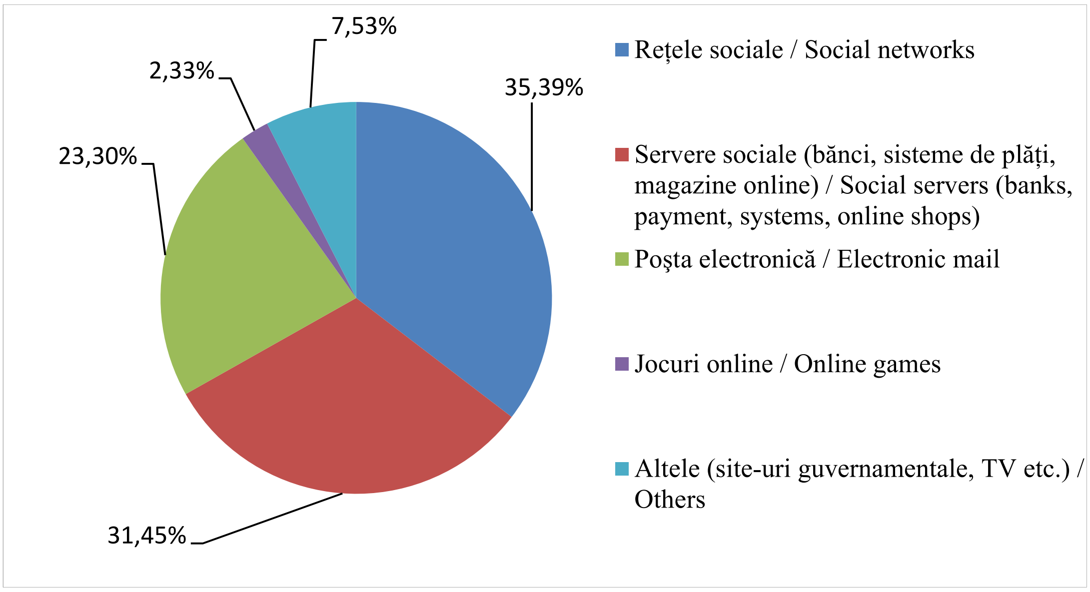


Figura 3. Scopul atacurilor phishing după tipuri în 2013 /
Figure 3. The objectives of phishing attacks according to types in 2013

Scopul atacurilor electronice

Comparativ cu anul 2012, împărțirea scopurilor după tipuri s-a schimbat considerabil. Cota atacurilor cu utilizarea paginilor false s-a mărit cu 6,79%, ajungând până la 35,39%, cota atacurilor financiare a crescut de la 8,5%, până la 31,45%. Cu toate acestea, s-a micşorat cota atacurilor cu utilizarea serviciilor poştale false – de la 10,5% până la 23,3%, a jocurilor online de la 3,14%, în 2012, până la 2,33%, în 2013.

The purpose of electronic attacks

It's noteworthy that in comparison with 2012 the parcelling of objectives according to types seriously changed. A percentage of attacks with use of fake social network pages increased from 6,79 % till 35,39%, the percentage of financial attacks- from 8,5% till 31,45%. The percentage of attacks with use of fake post services sites decreased from 10,5% till 23,3% and online games- from 3,14% in 2012 till 2,33% in 2013.

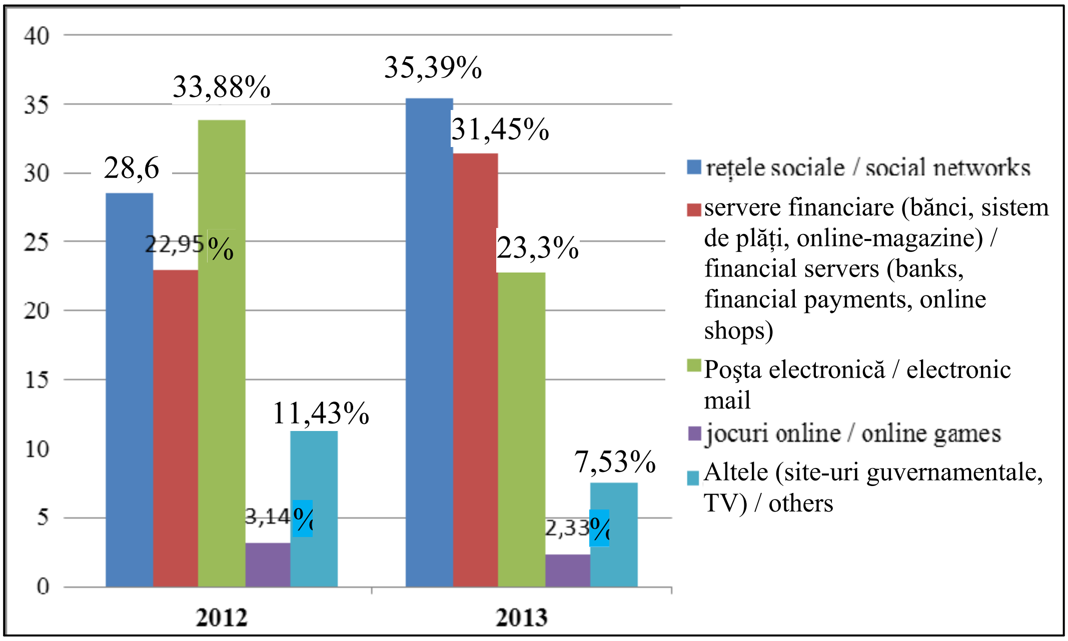


Figura 4. Scopul atacurilor phishing după tipuri în 2012 şi 2013/
Figure 4. The objective of phishing attacks according to types in 2012 and 2013

Este evident că anul 2013 se deosebeşte de 2012 prin sporirea atacurilor financiare, care invocă o analiză mai detaliată a dinamicii unor astfel de atacuri.

Atacuri phishing: tendință periculoasă

În anul 2012, din 22,95% phishing atacuri asupra diferitelor servicii financiare – 11,92% atacuri au întrunit falsificatorii site-urilor bancare şi sistemelor online banking; 5,66% au revenit site-urilor de internet-magazine şi 5,37% site-urilor de plăți.

It's obvious that 2013 stands out from the 2012 through increasing of financial attacks, claiming a more detailed analysis of the dynamics of such attacks.

Phishing attacks: a dangerous tendency

In 2012 out of 22,95% phishing attacks came to various financial services – 11,92% of attacks related to bank sites and online-banking systems falsification; 5,66%-online shop sites and 5,37% - payment system sites.

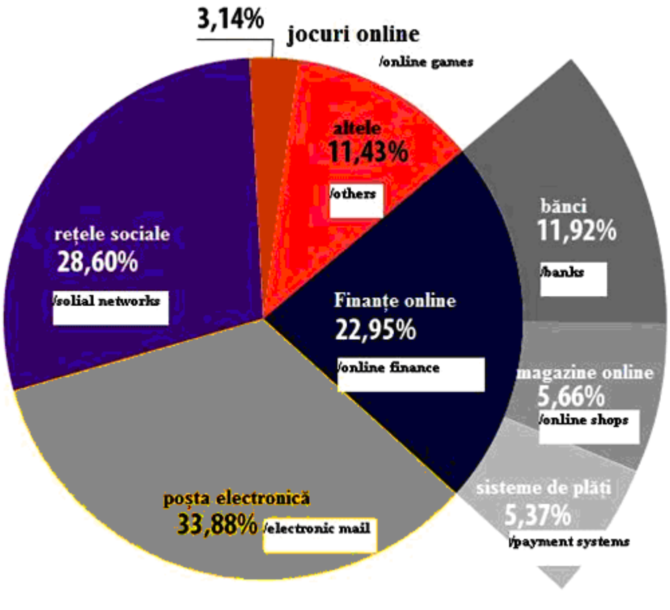


Figura 5. Atacuri financiare phishing în 2012 /
Figure 5. Financial phishing attacks in 2012

În anul 2013, la împărțirea atacurilor, în sistemul online, au apărut schimbări considerabile. Cota phishing îndreptată asupra băncilor s-a mărit dublu – până la 22,2%, puțin s-a mărit cota internet-magazinelor – de la 5,66% până la 6,51%, iar cota sistemelor de plăți s-a micşorat la 2,63%. De aici, rezultă că răufăcătorii atrag atenția mai des la paginile web bancare, tendința aceasta fiind una dintre cele mai solicitate ale sferei phishing-pericolului.

However, in 2013 allocation of attacks within online finance category faced considerable changes. A percentage of phishing aimed to banks increased almost in twice - till 22,2%, percentage of online shops – increased from 5,66% till 6,51%, but percentage of payment systems decreased to 2,63 %. The conclusion is obvious that the malefactors more often pay attention to bank web-services, this tendency is one of the most of strongly marked ones in the sphere of phishing-threats.

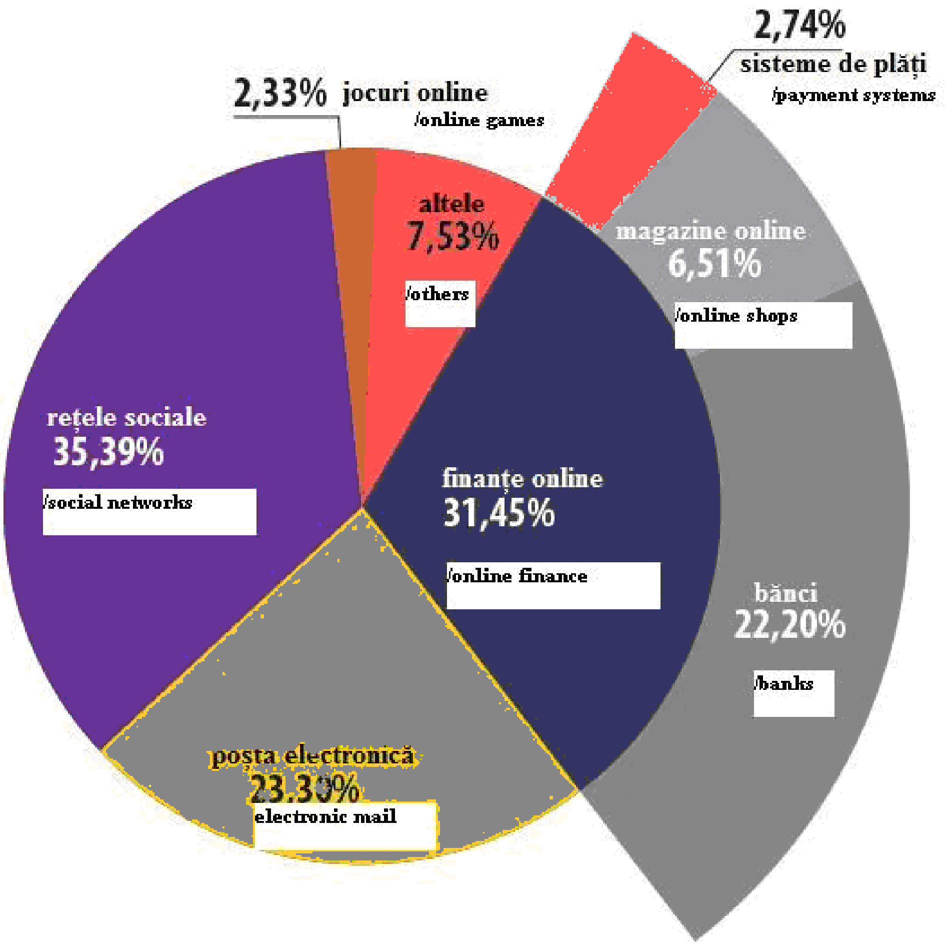


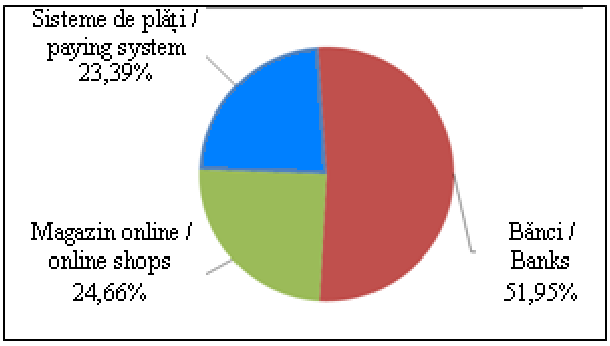
Figura 6. Atacuri financiare phishing în 2013 /
Figure 6. Financial phishing attacks in 2013

La fel, dacă este cazul să examinăm phishing-ul financiar aparte, de toate celelalte categorii, observăm că paginilor false ale băncilor le-au revenit 7,59% din toate paginile web anti-phishing. În analiza efectuată de „Laboratorul Kaspersky", în categoria online finanțe, cu un an mai înainte, cota phishing-ului bancar, în lista pericolului phishing financiar, era de 51,95%.

Cota atacurilor magazinelor online s-a micşorat de la 24,66%, în 2012, până la 20,71%, în 2013, iar cota atacurilor asupra sistemelor de plată a scăzut de la 23,39% până la 8,7%.

Another obvious tendency can be observed if we look at a financial phishing separately from all other categories,. there were 7,59% of fake bank pages of all web anti-phishing activations of "Kaspersky Laboratory" in the category online finance. Meanwhile, a year earlier, the percentage of bank phishing in general financial phishing threats was 51,95%.

The percentage of online shops decreased from 24,66% in 2012 till 20,71% in 2013, and the percentage of payment systems –from 23,39% till 8,7%.



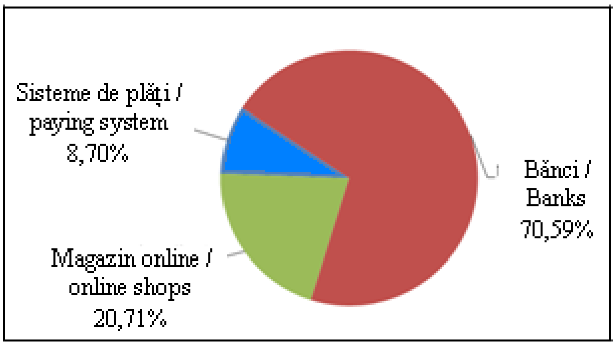


Figura 7. Phishing financiar în 2012 /Figure 7. Financial phishing in 2012

Phishing financiar în detalii. Băncile

În bazele anti-phishing, se conţin mai mult de 1000 de denumiri bancare, care au fost atacate din cauza popularităţii sau riscă să fie atacate de infractori în viitor. Majoritatea atacurilor phishing cu utilizarea paginilor false bancare, exploatau denumirea doar de la 25 de organizaţii, care lucrau în sfera bancară. Acestor 25 de bănci, în 2013, le-au revenit 59,5% din toate atacurile bancare, însă trebuie să atragem atenţia asupra faptului că o bună parte din denumirile incluse în lista dată sunt cele mai mari branduri bancare internaţionale, care lucrează în zeci de ţări din toată lumea. Reputaţia şi recunoaşterea pe piaţă a brandurilor constituie unul din principalele instrumente ale răufăcătorilor, care activează în phishing, întrucât, cu cât este mai popular brandul, cu atât îi este mai uşor infractorului să atragă utilizatorul pe un site fals.

Financial phishing in details. Banks

Though anti-phishing bases contain more than 1000 banks, which had been attacked or due to their popularity, risk to be attacked in future, the majority of all phishing attacks with use of fake bank pages, exploited denominations of only 25 organizations working in bank sphere. In 2013 for these 25 banks there were 59,5% of all bank attacks. Nevertheless, it needs to be mentioned that the suppressing part of this list are the greatest international bank brands working in dozens of countries all over the world. Recognition and popularity of brands is one of the major tools of malefactors practicing phishing, because the more popular a brand is, the easier is for malefactors to attract users on fake web sites with their names.

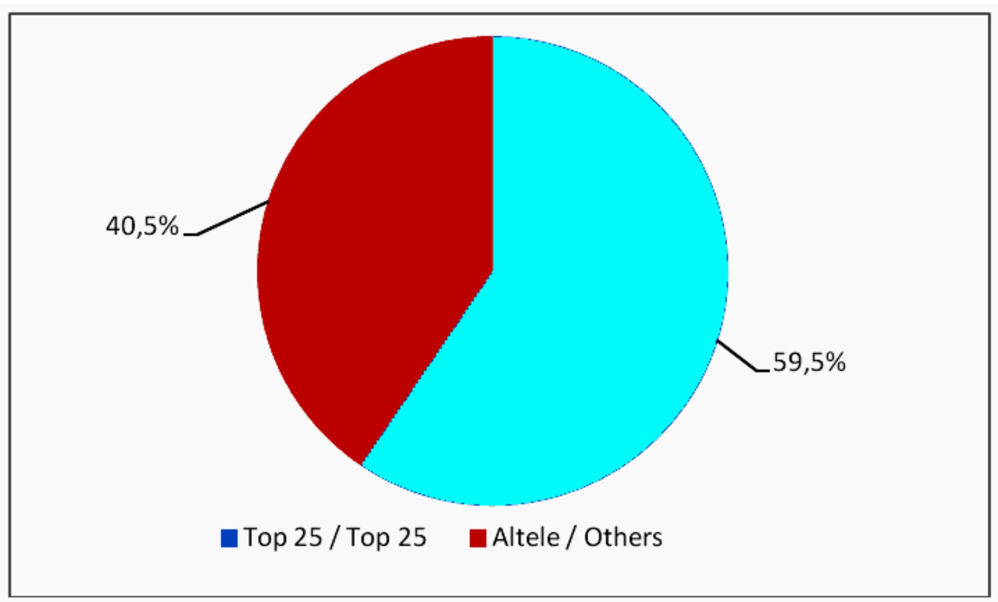


Figura 8. Atacuri cu utilizarea brandurilor de bănci în 2013 /
Figure 8. Attacks with usage of bank brands in 2013

Sisteme de plăţi

Ca şi în cazul atacurilor asupra băncilor, în repartizarea atacurilor asupra sistemelor de plăţi, un

Payment systems

Just as attacks on banks in the distribution of attacks on payment systems, a significant role is given rol semnificativ îl dețin recunoaşterea brandului – circa 90% din atacurile phishing împotriva sistemelor de plăți reveneau unuia dintre cele cinci branduri internaționale: PayPal, American Express, MasterCard International, Visa sau Western Union.

to brand recognition – about 90% of phishing attacks against incumbent payment systems are on five international brands: PayPal, American Express, MasterCard International, Visa or Western Union.

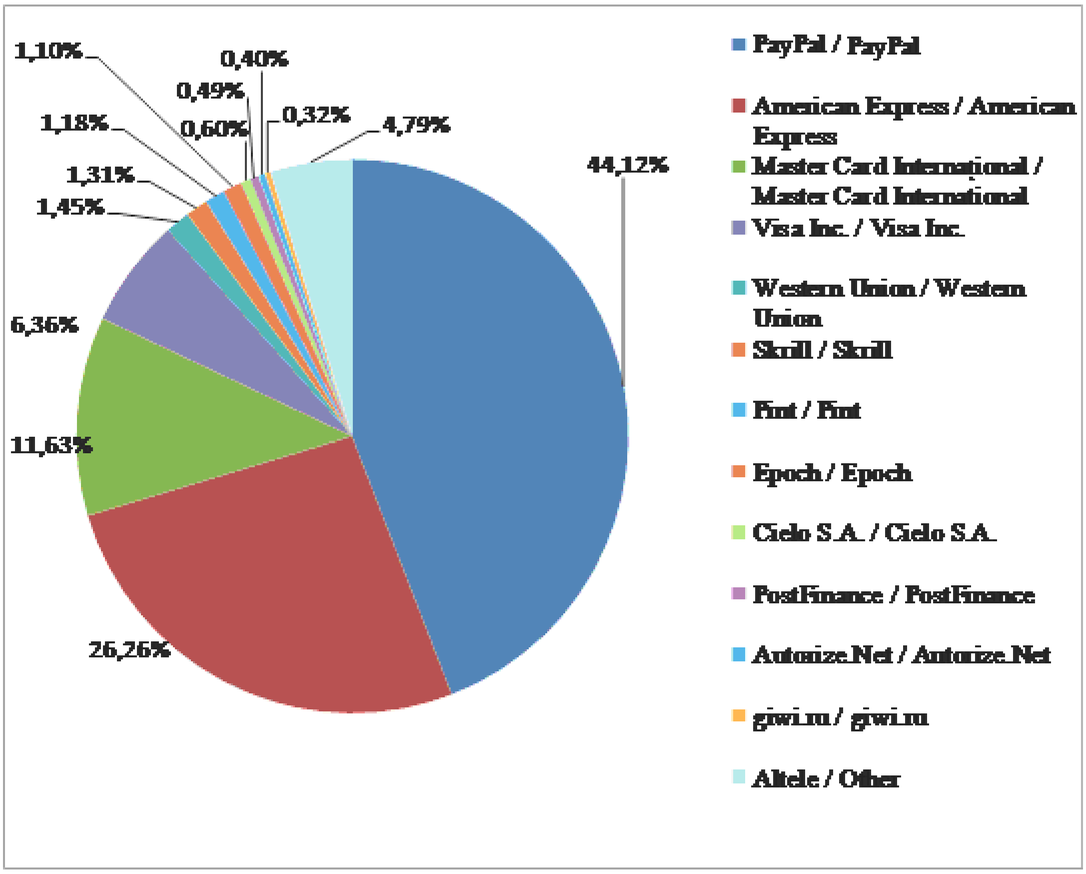


Figura 9. Atacurile asupra sistemelor de plăți, în 2013 /
Figure 9. Attacks against payment systems in 2013

PayPal, fiind excepțional de popular printre sistemele monetare de plăți în Internet, este foarte populară printre răufăcători – acest sistem a fost prejudiciat de circa 44,12% din totalul atacurilor.

O pondere semnificativă înregistra către American Express – 26,26%. Paginile sistemelor de plăți MasterCard International şi Visa Inc. sunt falsificate de atacatori mult mai rar, fiind atacate doar de 11,63% şi, respectiv, 6,36% tentative.

Magazine online

În categoria „magazine-online”, câțiva ani la rând, „lider” după numărul de atacuri sunt paginile phishing şi link-urile, în care se menționează internet-magazinul Amazon.com (61,11%).

Fiind cel mai mare magazin online din lume, cu o listă largă de produse, Amazon este cunoscut pentru mulți utilizatori şi, prin urmare, se bucură de popularitate printre hackerii care creează pagini false.

O proporție semnificativă (12,89%) o constituie atentatele la marca Apple, – de regulă, atacatorii

PayPal, being exceptionally popular among monetary payment systems in Internet, is very popular among malefactors – this system has accounted for about 44.12% of all attacks.

A significant percentage was at American Express – 26.26%. Payment systems pages of MasterCard International and Visa Inc. are falsified by attackers much rarely, being attacked only by 11.63% and 6.36% attempts.

Online shops

In the „online shops” category some years in a row the „leader” in attacks were phishing links and pages which remind of online shop Amazon.com (61,11%).

Being the largest online shop in the world, with an extensive product list, Amazon is known to many users and, therefore, enjoys popularity among hackers who create fake pages.

A significant proportion (12.89%) constitute breaches of the Apple brand - usually Internet attackers încearcă a simula internet-magazinele prin dispozitive Apple şi suplimentele App Store şi iTunes Store.

Atacuri cu menționarea celor mai populare magazine online în 2013

try to simulate the devices Apple and supplements App Store and iTunes Store.

Attacks mentioning the most popular online shops in 2013

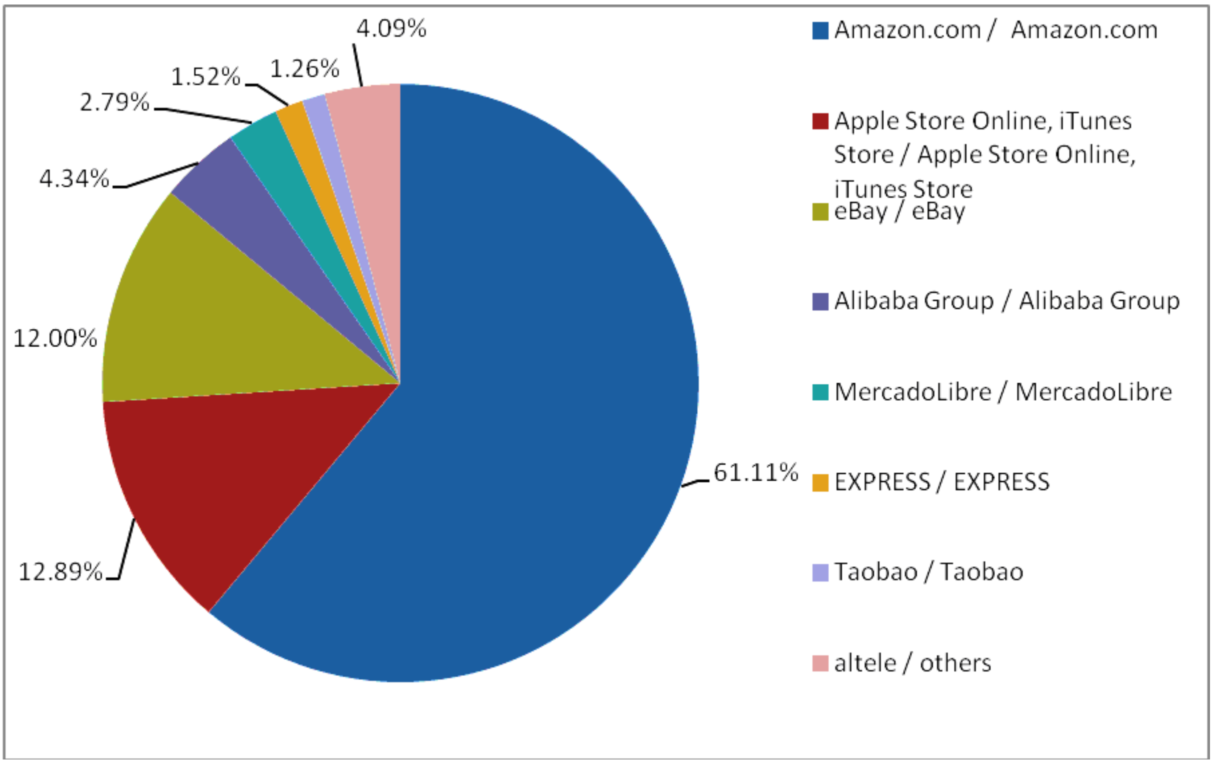


Figura 10. Dinamica atacurilor asupra magazinelor online în 2013 /
Figure 10. Dynamics of attacks ower online shops in 2013

Activitățile profesionale şi de marketing ale companiei, numele căreia este apoi utilizat în sistemele de atac tip phishing, influențează asupra numărului de atacuri în general.

În mod evident, această tendință este ilustrată prin atacurile, care folosesc numele companiei Apple şi produselor sale.

Printre obiectivele atacurilor, în mod tradițional, se înscriu Internet-licitațiile eBay (12%). Atacurilor frecvente este supus celebrul magazin online chinezesc – Alibaba (4,34%), şi, în plus, din 2013, la el s-a alăturat un alt magazin online chinezesc – Taobao (1,26%). Aproape 3% din toate atacurile asupra magazinelor online reveneau pentru MercadoLibre.com – analog eBay din America de Sud. Datele expuse în figura 10 ilustrează elocvent modul de repartizare (conform popularității brandului) a phishing-ul financiar „internațional”. După cum se poate observa, victime ale atacurilor pot fi nu numai utilizatorii vorbitori de limba engleză, dar şi oameni a căror limbă maternă este chineza, spaniola, portugheza etc.

Dinamica atacurilor în detaliu

Professional and marketing activities of the company, whose name is then used in systems phishing attack, influences the number of attacks.

Obviously, this trend is illustrated by attacks that use the name Apple and its products.

Traditionally, the targets of attacks are the eBay Internet-auctions (12%). Frequent attacks are committed against the famous Chinese online store Alibaba (4.34%), and in addition, in 2013 there had joined the other Chinese online store – Taobao (1.26%). About 3% of all attacks upon online shops referred to MercadoLibre.com – analogue for eBay from South America. This data is illustrated in figure 10, “International” financial phishing.

As it can be seen, the victims of the attacks can be not only English-speaking users, and people whose native language is Chinese, Spanish, Portuguese, and others.

Dynamics of attacks in details

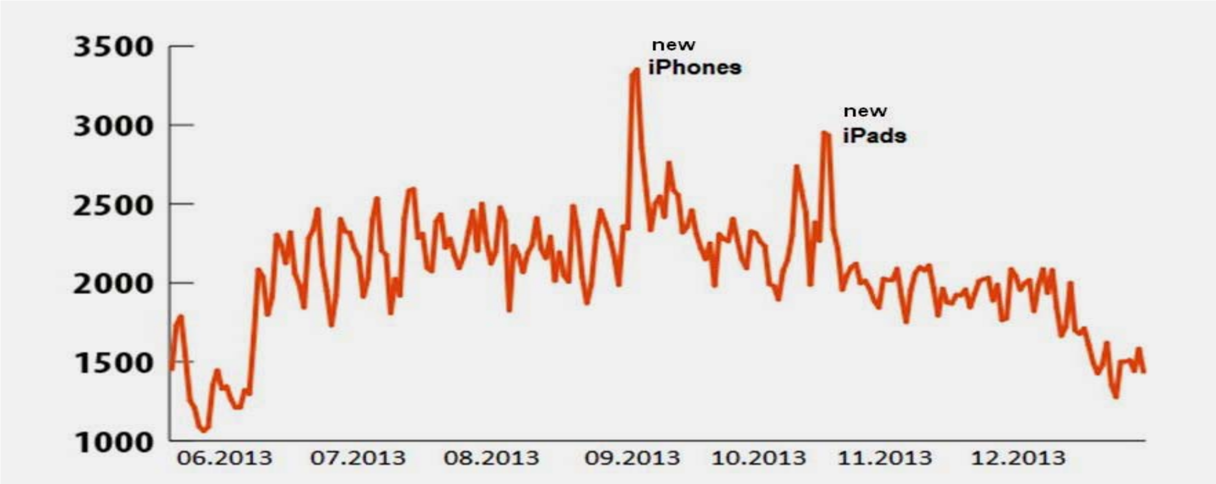


Figura 11. Atacurile asupra brandului Apple în semestrul al II-lea al anului 2013 / Figure 11. Attacks using the Apple brand in the second part of 2013

Pe parcursul anului, dinamica de reacţionare şi apărare a tehnologiilor „Laboratorului Kaspersky" asupra pericolelor care exploatează marca Apple au demonstrat un şir de căderi de la 1 până la 2,5 mii de reacţionări pe zi, însă, după cum se observă în graficul de mai sus, în istoria atacurilor au fost două puncte maximale care, după date, coincideau cu lansarea smartphone-urilor Iphone 5S şi 5C, din 10 septembrie 2013 şi a planşetelor Ipad Air şi Ipad mini, din 22 octombrie 2013.

Este ceva logic şi clar, deoarece tehnica Apple reprezintă întotdeauna, o temă fierbinte în noutăţi şi în discursurile din internet, iar, în perioada lansării produselor noi, îndeosebi. Pentru răufăcători, utilizarea cuvintelor-cheie este o metodă obişnuită de atragere a auditoriului pe site-ul fals şi, după cum se vede în grafic, metoda funcţionează.

Apple nu constituie unicul scop al fişierelor (programe informatice menite a dăuna), numărul atacurilor şi al brandurilor se schimbă în funcţie de activitatea companiilor de marketing.

Concomitent cu cataclismele naturale, cu noutăţile importante şi cu informaţiile internaţionale, care sunt relatate în SMI şi discutate în internet, apar imboldurile pentru apariţia aşa-numitului phishing tematic şi al spamului. Astfel, băncile, internet-magazinele, companiile de marketing ori alte companii financiare pot avea motiv de phishing.

Phishing împotriva utilizatorilor OSX

Primele simptome ale pericolului de creştere a atacurilor asupra posesorilor de calculatoare, sub conducerea sistemelor de operare OSX, tot timpul, au fost de câteva ori mai joase decât împotriva Windows utilizatorilor, fapt care se explica simplu, deoarece Apple activează şi lansează calculatoarele şi note-bookurile Mac în toate ţările lumii. Numărul utilizatorilor de asemenea calculatoare nici nu se compară cu numărul utilizatorilor PC în Windows. Din dorinţa de a obţine venituri maximale, răufăcătorii îşi îndreaptă atenţia către utilizatorii windows, cu toate că acestea au loc când este vorba de programe virulente. Infractorul nu trebuie să facă nimic deosebit, ca să atace

During almost the whole year the dynamics of activities of "Kaspersky Laboratory" security technologies against threats exploiting market brand Apple represented a raw of rises and falls within 1 and 2,5 thousand activities per day, however as it is seen on the graphic above the history of attacks had two significant turning points, which exactly coincided with date of the announcement of smartphone iPhone 5s and 5c (10th September 2013) and tablets iPad air and iPad Mini with retina display (22nd October 2013)

The logic in this case is clear: Apple technology is always a breaking topic for news and Internet discussions and, especially, on the eve of new products announcements. For malefactors usage of "hot" key words is an ordinary way of attracting audience on phishing sites and as it's seen on the graphic, this method works.

Apple is not the only target of phishers, number of attacks of which changes depending on the company's marketing activity.

Together with natural disasters and grand international events an active showing of which gives a push for appearing so called thematic phishing and spam in Mass Media and Internet. An altitudinous marketing bank company, online shop or any other market or financial organization can be a motive for phishing.

Phishing against OS X users

The number of maleficent attacks to users of computers under guidance of Software OSX has always been several times lower than number of attacks against Windows users. That can be easily explained: although Apple actively promotes its computers and Mac notebooks in countries all over the world. The number of users of such devices does not go in comparison with number of Windows users.

Guided by aspiration to gain maximum profit the criminals therefore pay more attention to Windows users. Nevertheless this statement is fair enough only when talking about deleterious programs. The malefactor doesn't need to do anything special to attack utilizatorul Mac cu ajutorul phishing-ului, deşi sistemele operaţionale windows şi OSX au deosebiri principiale, care nu permit scrierea universală la ambele platforme ale utilizatorului PC şi Mac. Ei utilizează unele şi aceleaşi web pagini, astfel, metodele de pericol phishing pentru utilizatorul Mac sunt mai actuale decât pentru utilizatorul PC. Rezultatele cercetării „Laboratorului Kaspersky" au demonstrat acest fapt. Numai că, înainte de a face vreo însemnare din cauza defecţiunilor tehnice, „Laboratorul Kaspersky" are să adune o statistică relevantă de la utilizatorii Mac. Cercetările efectuate şi informaţia despre Mac, selectată începând cu luna noiembrie până în decembrie 2013, deşi perioada nu este mare, oricum datele permit să ne facem o imagine despre proporţiile pericolului ce-i pândeşte pe utilizatorii OSX şi să observăm care este diferenţa în tabloul comun. Astfel, în 2013, 7,8% dintre atacurile recepţionate de tehnologiile de apărare ale „Laboratorului Kaspersky" au avut loc asupra produselor companiei de apărare a calculatoarelor Mac. Majoritatea atacurilor au fost săvârşite asupra utilizatorilor din SUA 47,55%; 11,53% din atacuri au fost înregistrate în Germania; 5,47% – în Anglia, iar cele mai puţin atacate ţări sunt, la etapa actuală, Canada şi Australia.

Zile de atacuri intensive phishing:

(Bazate pe date din septembrie 2011-septembrie 2012)

1. Vineri (38,5%)
2. Luni (30%)
3. Duminică (10,9%)
4. Joi (6,5%)
5. Marţi (5,8%)
6. Miercuri (5,2%)
7. Sâmbătă (3,2%)

a Mac user with phishing, because though Windows software and OSX have principled differences not allowing writing universal deleterious Software for both of platforms, PC and Mac users load the same web-pages and phishing threats spread by means of social engineering, equally actual for Mac and PC users. The research results of "Kaspersky Laboratory" had confirmed this fact. Although first of all an important remark be mentioned: because technical reasons "Kaspersky Laboratory" has a possibility to collect relevant stats from Mac users only from November 2013 and all information regarding Mac used in this research is collected within period from November till December 2013. Though the outlook period is not great, the data got during this period allow getting some representation about threats landscape for OSX platform users and point out the differences between this and "general" picture of it. In 2013 7,8% of activated security technologies of "Kaspersky Laboratory" had happened onto products of Mac company for computers security. Almost half of all attacks were directed on USA users (47,55%), 11,53% were fixed in Germany, 5,47% in Great Britain. Sweden and Australia also appeared in the top attacked countries list.

Days of intensive attacks

(Based on September 2011-September 2012 research)

1. Friday (38.5%)
2. Monday (30%)
3. Sunday (10.9%)
4. Thursday (6.5%)
5. Tuesday (5.8%)
6. Wednesday (5.2%)
7. Saturday (3.2%)

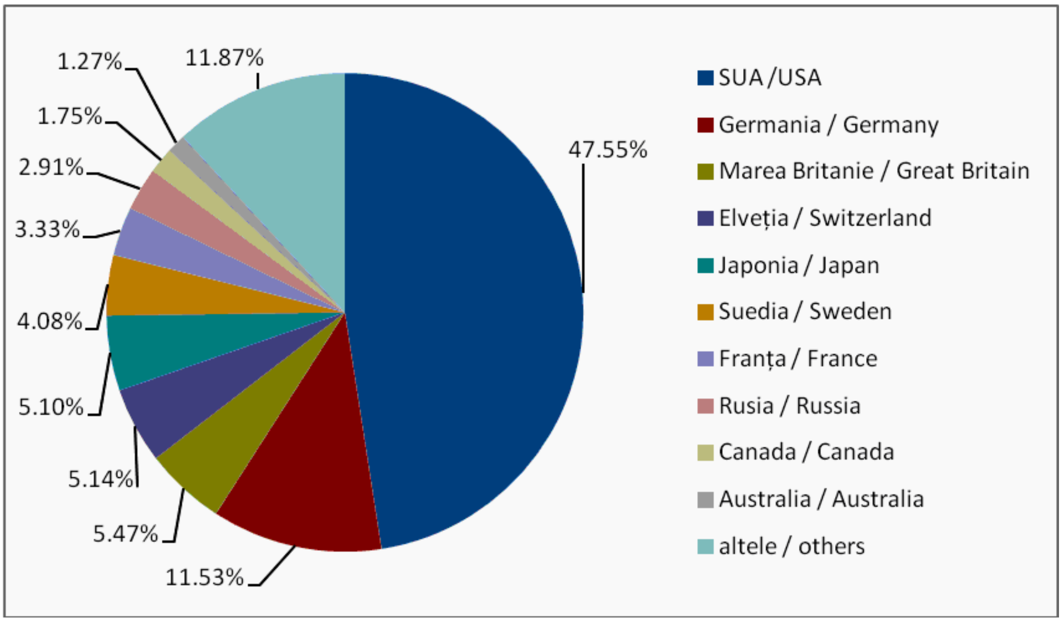


Figura 12. Dinamica celor mai atacate ţări: Utilizatorii Mac /
Figure 12. The most frequently attacked countries: Mac users

Diferența dintre nivelurile de atac asupra sistemelor informaționale din diverse țări ale lumii se poate explica prin faptul că, în aceste țări, sunt mai răspândite calculatoarele Apple. De regulă, SUA şi alte țări europene dezvoltate sunt cele mai mari piețe de desfacere a produselor companiei Apple.

În perioada analizată de „Laboratorul Kaspersky", aproximativ 38,92% din toate atacurile web anti-phishing au avut loc prin intermediul paginilor phishing ale calculatoarelor Apple, ce e aproape cu 7,5% mai mult decât cota financiară generală din mărimea atacurilor. Majoritatea incidentelor au avut loc între utilizator şi site-urile bancare false – 29,86%, în timp ce asupra magazinelor online şi licitațiilor – 6,6%, iar asupra sistemelor de plăți – 2,46%.

The differences in attacks allocation to countries can be explained with a wider spreading of Apple computers mainly in these countries. Traditionally USA and developed European countries are the largest sales markets of Apple technology.

During period of research circa 38,92% of all web-anti phishing activations of "Kaspersky Laboratory" on Apple computers were financial phishing pages, which is almost with 7,5% more than "financial" percentage in general attacks content. Herewith the majority of incidents – 29,86% were users' facing bank phishing sites, meanwhile online shops and auctions had – 6,6% activations and payment systems – 2,46%.

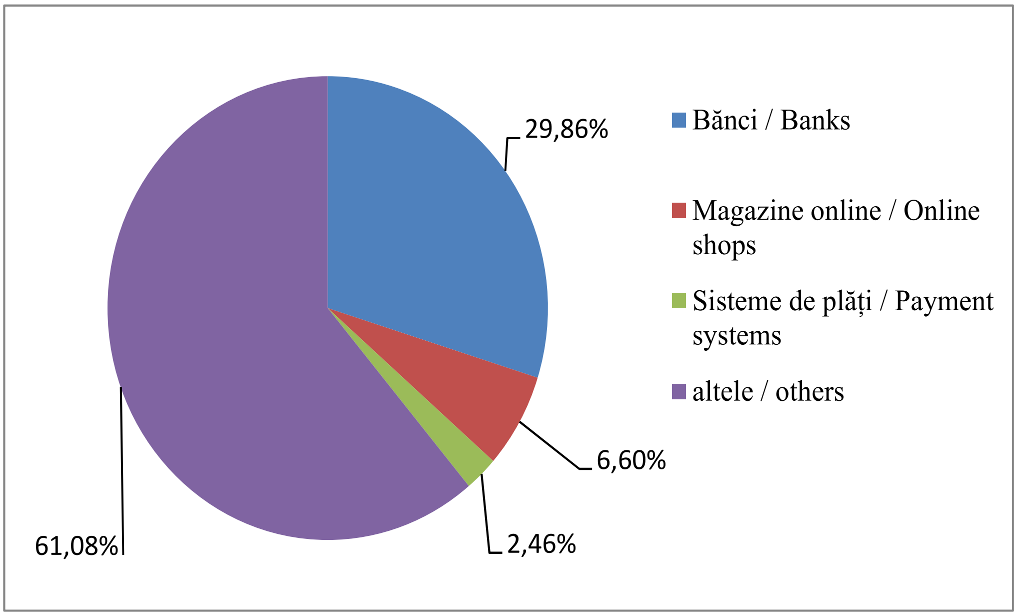


Figura 13. Phishing financiar: atacurile împotriva utilizatorilor Mac / Figure 13. Financial phishing: attacks against Mac users

Cifrele arată că proprietarii de Mac se confruntă cu atacuri de tip phishing la fel de des ca şi utilizatorii de PC-uri pe Windows, iar probabilitatea de a deveni o victimă a atacurilor financiare este chiar mai mare.

Concluzii

Deşi phishing-ul continue să se răspândească, în ciuda eforturilor de limitare a fenomenului, devenind o amenințare serioasă la nivel global, atunci când vine vorba de cyber-criminalitatea financiar-informatică, aceasta reprezintă doar o parte relativ mică din peisajul financiar general al amenințărilor cibernetice. Un rol important, în acest domeniu, îl joacă un malware financiar – programe software periculoase, care pot, în mod camuflat pentru utilizator, să dobândească informații, rechizite online pentru acces la datele confidențiale, la conturile bancare personale ale acestuia şi chiar să fure banii victimei.

The numbers show that Mac owners face phishing attacks as much often as Users on PC with Windows but possibility to become a financial attack victim is even higher.

Conclusions

Although phishing is quite a common threat when it comes to financial, computer cyber-crime it is only a relatively small proportion of the global financial landscape of cyber-threats. An important role in this field is played by a financial malware – dangerous software that can camouflage for the users to acquire information, supplies online access for accounts and even steals money of the victim.

Bibliografie / Bibliography:

1. BĂDĂRĂU, E., GRIBINCEA, A. *Problemele juridice privind folosirea numelui de domeniu în Internet*. Conferinţa internaţională ştiinţifico-practică „Inovarea în susţinerea întreprinderilor mici şi mijlocii", 27-28 noiembrie 2008, Chişinău: AGEPI, 2008, p. 56-59
2. GRIBINCEA, A. *Relaţii economice internaţionale: multimedia, cibermarketing şi Internet*. Chişinău: *ULIM,* 1999, 82 p.
3. http ://www .cbronline. com /blogs/ cbr-rolling-blog/websense-says-educating-employees-will-help-stop-phishing-attacks-091012
4. http ://www .microsoft .com /ru -ru/security/online-privacy/phishing-symptoms.aspx
5. http ://www .microsoft .com/ ru-ru/security/online-privacy/information.aspx
6. http ://www .solovatsoft .com /OEM_Spam_Filtering_Engines.html
7. https ://safety .yahoo .com /Security/PHISHING-SITE.html
8. https ://www .onguardonline .gov /phishing
9. https ://www. nsslabs .com /reports/ consumer -avepp-comparative-analysis-phishing-protection - edition-1