MODALITĂȚI DE PREVENIRE ŞI COMBATERE A FRAUDELOR INFORMATICE ÎN REGIM TRASFRONTALIER

Teodor Bivol, prof.
Preşedinte al Asociației Cultural-Ştiințifice "Vasile Pogor" din Iaşi – România

Frauda informatică este întotdeauna un act premeditat. - Teodor Bivol

Abstract. The purpose of this article is to attention about the risks coming from using information technologies. The main point is to notice the main risk factors in information infractions, to identify their subjects and motivation, to establish efficient and effective security measures. Because even now, in the top of Information Age, these risks are not treated properly, things that in the end can cause not only financial lost.
Cuvinte cheie: Fraudă informatică, skimming, phishing, malware, mesaj electronic.

Frauda informatică reprezintă un fenomen al zilelor noastre. Psihologii spun că teama de atacuri informatice o depăşeşte în intensitate pe cea faţă de furturi sau fraude obişnuite.

În condiţiile în care doar 5% dintre faptele penale săvârşite prin utilizarea sistemelor informatice, ajung la cunoştinţa organelor de cercetare penală, am consideat necesar să conştientizăm tot mai mult efectul numit:
fraudă informatică.

Potrivit Inspectoratului General al Poliţiei Romane – Brigada pentru Combaterea Crimei Organizate, în prima jumătate a anului 2012 fraudele cu carduri au cunoscut o creştere exponenţială, înregistrându-se numeroase cazuri de persone depistate la bancomate în Romania care folosesc cărţi de credit în mod fraudulos. De asemenea, autorităţile străine au semnalat numeroase cazuri în care cetăţeni români sunt depistaţi comitând astfel de fraude la bancomate în afara ţării. În cele mai multe cazuri, activităţile infracţionale sunt iniţiate din Romania dar vizează victime din străinătate sau sunt finalizate în străinătate, unde se ridică produsul financiar.

Autorii folosesc în comiterea acestor fapte sisteme de plată rapide oferite prin Internet (sistem escrow, conturi de paypal, conturi e-gold, conturi de internet - bancking) sau sisteme de transfer rapid de bani (wire transfer – servicii oferite de instituţii ca Western Union sau Money Gramm).

Cele mai active zone ale ţării, în ceea ce priveşte comiterea acestui gen de fapte sunt: Bucureşti, Alexandria, Râmnicu Vâlcea, Craiova, Timişoara, Iaşi, Sibiu şi Constanţa.

Conform rapoartelor IGPR, se remarcă o tendinţă de specializare continuă a infractorilor atât asupra activităţilor desfăşurate, cât şi din punct de vedere tehnic, pentru identificarea de noi moduri de operare: licitaţii frauduloase, folosire de site-uri false de escrow, site-uri de transport, site-uri de comerţ electronic, site-uri de phishing, ascunderea urmelor prin Internet şi a circuitului produsului financiar.

Din cazuistica instrumentată de IGPR, reiese faptul că o parte din reţelele criminale organizate, transnaţionale, care în trecut îşi desfăşurau activitatea în alte domenii (trafic de autoturisme furate, trafic de fiinţe umane şi chiar traficul de droguri) s-au reorientat, săvârşind infracţiuni cu cărţi de credit şi prin INTERNET, sumele de bani obţinute în mod ilicit ca urmare a acestor activităţi fiind uneori mult mai mari decât cele obţinute anterior.

Factorii care au determinat reorientarea grupărilor criminale către infracţiuni cu cărţi de credit sunt:

- obţinerea de câştiguri materiale mari într-un timp relativ scurt şi cu riscuri relativ mici;
- caracterul transfrontalier al infracţiunilor face ca instrumentarea acestora de către autorităţile unui stat să fie mult mai dificilă, întrucât pentru probarea faptelor este nevoie, de cele mai multe ori, de obţinerea unor informaţii de la autorităţile competente din mai multe state, pe calea cererilor de asistenţă juridică internaţională, procedură ce este costisitoare şi lentă;
- accesul facil la echipamente moderne, care permit desfăşurarea de activităţi ilicite complexe;
- posibilitatea deplasării rapide de pe teritoriul unui stat pe teritoriul altui stat a membrilor unei grupări criminale, urmărirea activităţii desfăşurate de către aceştia fiind de cele mai multe ori, foarte greu de realizat de către autorităţile competente.

La nivelul Direcţiei Generale de Combatere a Criminalităţii Organizate, a fost înfiinţat un compartiment specializat în domeniul prevenirii şi combaterii pornografiei infantile, dată fiind importanţa Internet-ului, ca şi mijloc de comunicare, în special în rândul tinerilor. În ceea ce priveşte cimininalitatea în domeniu, nu se înregistrează evoluţii semnificative nefiind depistate sau semnalate cazuri de racolare de minori prin Internet, care, ulterior, să fie victime ale unor abuzuri sexuale. În schimb, se înregistrează un număr crescut de cazuri în care tineri, elevi sau studenţi se filmează în timpul unor acte sexuale, după care distribuie materialele prin Internet.

Pentru a asigura o ripostă eficientă acestui gen de fapte infracţionale, Direcţia Generală de Combatere a Criminalităţii Organizate a pus bazele unui task-force cu F.B.I., pe linia fraudelor informatice, care, începând cu luna aprilie 2011, a devenit operaţional şi desfăşoară activităţi specifice de investigare. Primele şase luni ale anului 2011, relevă faptul că au fost constatate 526 de infracţiuni comise în domeniul criminalităţii informatice. Din cele 340 de persoane învinuite, 65 au fost reţinute sau arestate.

Cooperarea la nivel internaţional cu Poliţii din alte state, precum şi coordonarea activităţilor desfăşurate de autorităţile române şi străine, au condus la destructurarea mai multor reţele infracţionale. De exemplu:

- „Operațiunea Brăila", desfășurată în colaborare cu autoritățile polițienești din Spania, împotriva unei grupări infracționale alcătuită din cetățeni români, ce acționau în special în România și Spania, dar care aveau ramificații în mai multe state europene precum Belgia și Franța;

- "Operațiunea Armaghedon" a fost demarată în luna septembrie a anului 2010 de către Brigada Centrală de Investigații și Delincvență Specializată din Spania, la succesul acesteia contribuind polițiști spanioli, români și italieni, sprijiniți de Interpol și Europol. În cadrul acesteia, o rețea de falsificatori de carduri a fost anihilată de către polițiștii români în colaborare cu autorități din alte state, fiind arestate 14 persoane în România și 65 în Spania. Grupul infracțional era specializat în producerea de echipamente pentru contrafacerea de cărți de credit cu care, ulterior, se realiza extragerea banilor din bancomate, atât în România cât și în țări din vestul Europei: Italia, Spania, Olanda, Danemarca, Suedia, Franța;

- „Operațiunea Clone" care prin colaborare cu autoritățile italiene a dus la arestarea, în Italia, a 14 persoane;

- „Operațiunea Savitar" desfășurată în colaborare cu autoritățile daneze a facut ca 24 de persoane să fie arestate în Danemarca și Olanda.

În primul semestru al anului curent, structurile centrale și teritoriale ale Direcției de Combatere a Marii Criminalități Economico - Financiare au constatat 1.131 infracțiuni, fiind cercetate 540 de persoane, printre care și un minor, 44 dintre acestea în stare de reținere sau arest.

Din cele 540 de persoane, 58 au fost cetățeni straini. Polițiștii Direcției au mai identificat 42 de grupuri infracționale, dintre care au fost anihilate opt și au confiscat 21.263.580 de euro, 150.000 de USD, două milioane de RON, șapte autoturisme, 26 de imobile, 2,681 kg. de aur, precum și bunuri în valoare de 124.000.000 de RON.

Modalitățile de spălare a banilor folosite de către infractori sunt, cel mai adesea: spălarea banilor obținuți din contrabandă și evaziune fiscală, prin intermediul sistemului bancar, de către grupuri infracționale organizate, specializate în înființarea și folosirea firmelor fantomă, pentru a transfera ilegal în străinătate fondurile obținute din astfel de activități ilegale, transferarea succesivă a unor mari sume de bani, din conturile curente ale societăților comerciale ce desfășoară activități aparent legale, în contul unor firme fantomă, pe baza unor operațiuni comerciale fictive (asistență, consultanță, prestări servicii), diminuând astfel baza impozabilă și generând fictiv TVA deductibil, crearea de circuite financiare și comerciale fictive prin folosirea de societăți de tipul fantomă pentru obținerea de rambursări ilegale de TVA sau prin utilizarea unor documente comerciale falsificate, care proveneau de la societăți comerciale fantomă, mulți infractori au solicitat și obținut rambursări ilegale de TVA și compensări cu obligații fiscale.

O altă metodă este spălarea banilor, de regulă, prin utilizarea firmelor și băncilor din "paradisurile fiscale", folosindu-se „inginerii financiar bancare" specifice.

Pentru documentarea infracțională a grupărilor criminale din sfera criminalității organizate, a contrabandei cu produse contrafăcute, precum și a contrabandei cu tutun dar și pentru combaterea spălării banilor, a fraudelor fiscale și a infracțiunilor la regimul pieței de capital, concomitent cu instituirea măsurilor asiguratorii, în vederea confiscării bunurilor și valorilor folosite sau obținute prin săvârșirea de infracțiuni legate de criminalitatea organizată au fost constituite de grupuri de lucru comune de către Parchetul de pe lângă Înalta Curte de Casație și Justiție - Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism, Oficiul Național Pentru Combaterea Spălării Banilor, Garda Financiară, A.N.A.F. și A.N.V

Sau pentru monitorizarea afacerilor ilegale cu petrol, în special în zona Portului Constanța.

Principalele moduri de operare întâlnite sunt:[1]

- ***SKIMMING-ul*** care constă în instalarea de dispozitive la bancomate, POS-uri sau camere de luat vederi prin care sunt copiate datele de pe benzile magnetice ale cardurilor și este capturat PIN-ul. Ulterior, datele obținute sunt transferate în computere și, cu ajutorul altor dispozitive, banda magnetică a cardului este reinscripționată.

- ***PHISHING-ul*** - crearea unor pagini web false și transmiterea de mesaje electronice către diverse persoane în scopul obținerii unor date de identitate sau informații confidențiale de pe carduri sau referitoare la conturi bancare.

-***MALWARE***[2]-ul, ca orice alt produs informatic, a suferit o serie de schimbări (o evoluție) de-a lungul timpului. Dacă inițial, malware-ul avea un caracter demonstrativ (în sensul că marea majoritate a creatorilor de malware încercau să demonstreze că pot crea un malware foarte complicat de detectat), o dată cu evoluția internetului, malware-ul a capătat un aspect tot mai comercial.

În ultimii 2 ani, creatorii de malware se orientează tot mai mult spre câștiguri financiare cât mai mari și mai rapide. Acest lucru a schimbat nu doar forma malware-ului ci și metodele de diseminare a acestuia. Încep să fie tot mai prezenți malware de tipul adware și spyware, rețelele de boți cresc tot mai mult, apar tot mai multe atacuri bazate pe diverse tipuri de vulnerabilități (cele mai multe browser-based).

- ***„Social engineering-ul"*** este tot mai utilizat ca și metodă de câștig financiar, fie direct prin spam-uri, fie indirect pentru a facilita diverse metode de diseminare a malware-ului. Apar și categorii noi de amenințări informatice: rogue / fake antiviruși. Începe să apară și o diferențiere tot mai clară la nivel global în ceea ce privește diseminarea diverselor tipuri de malware. Cei cu câștig rapid (adware, rogue-uri av) sunt diseminați în special în zonele în care profitul financiar poate fi obținut rapid (de exemplu Statele Unite / Canada). Celelalte tipuri de malware (cele bazate pe vulnerabilități sau spyware-ii) sunt mai prezenți în China, Rusia, etc.

Metodele principale de diseminare a malware-ilor sunt drive-by-download, tehnici black-seo, e-mail, serviciile de instant messange-ing cum ar fi Yahoo Messenger, Skype

---

[1] Prelucrare după: http://www.prevenire-fraude.ro/

[2] Un software care a fost creat într-un scop malițios (fie pentru distrugerea datelor dintr-un calculator, fie pentru modificarea și / sau furtul unor informații secrete, fie ca metoda de control a unui calculator) toate acestea fără consimțământul userului.

sau diverse vulnerabilități care puteau fi exploatate la browsere. Alte metode des utilizatate sunt programele P2P (Ares, BearShare, iMesh, Shareza, Kazaa, DC++, eMule, LimeWire) precum și torentele.

Terminologie:

- ***Adware*** – este un program care afișează diverse tipuri de reclame (fie în fereastra proprie fie în ferestre de tip pop-up). De multe ori, lucrează cu un server care îi servește reclame noi. Câștigurile financiare provin direct de la furnizorii pentru care se face reclamă. În cele mai multe cazuri, avem de a face cu adware foarte agresivi (de exemplu, care îți afișează o fereastră cu reclame pe ecran și nu te lasă să rulezi aplicația originală o perioadă de timp).

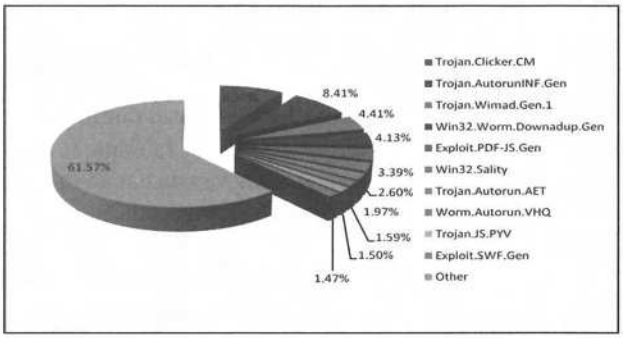
- ***Browser modifier***[3] – constă în diverse componente (ActiveX, BHO, etc) care modifică modul în care un browser funcționează. De cele mai multe ori, modifică rezultatele diverselor căutări (fie propulsând anumite rezultate în față, fie renunțând la unele).

- ***Spyware*** – într-o terminologie mai generală, se referă la o aplicație care stochează și trimite date confidențiale de pe calculatoarele pe care rulează. De cele mai multe ori, aceste date confidențiale sunt parole, conturi de e-mail sau pentru alte servicii, diverse date legate de credit cardurile utilizate pe utilizator. De obicei, informațiile culese sunt utiliate, fie pentru a folosi acele conturi de email pentru a trimite SPAM-uri, fie pentru a fura alte informații (dacă parolele furate sunt de la acel calculator). Chiar dacă nu este considerat o forma de spyware, phishing-ul funcționează într-un mod similar: anumite pagini de web (de obicei pagini care să necesite introducerea de date personale) sunt clonate și modificate astfel încât datele personale sunt trimise către atacator.

- ***Fake/Rogue AV/Scareware.*** E un tip nou de malware, care folosește tehnici de „social-engineering" ca să convingă un utilizator să cumpere un anumit produs. Mecanismul este simplu și eficient. Printr-o anumită metodă (drive-by-download, email, vulnerabilități, etc) un astfel de program ajunge pe calculatorul victimei. La execuție, se comportă ca un AntiVirus tradițional (deci cu interfață, diverse posibilități de scanare / configurare). Singura diferență este că detectează foarte multe fișiere pe sistemul victimei ca fiind infectate cu malware inexistenți. După ce prezintă un astfel de raport fals userului, i se spune că produsul de față este freeware și nu are și posibilitate de dezinfecție. Însă, în schimbul unei sume de bani, userul poate cumpara varianta completă a produsului și să își dezinfecteze calculatorul. În ultima perioadă, aceste aplicații apar direct în cadrul browserului și folosind diverse scripuri JavaScript sau chiar obiecte flash simulează o scanare, prezentând o serie de rezultate false userului în vederea convingerii acestuia să downladeze și să execute diverse aplicații rogue ce aparțin atacatorului.

Tipuri de malware în anul 2012

Un raport BitDefender pentru anul 2012 arată urmatoarea repartizare a diverselor tipuri de malware în lume:



Dintre acestea:

- ***Trojan.Clicker.***CM este un script înserat în diverse pagini de web des utilizate (pagini ce găzduiesc keygen-uri sau crack-uri în special) și care afișează diverse reclame în browser.

- ***Trojan.AutorunINF sau varianta lui Autorun. AET*** sunt detecții generice pentru o metodă de răspândire foarte des utilizată de wormi (creare de fișiere autorun. inf ascunse pe foldere share-ate sau pe memory stick-uri și execuția lor automată în momentul locațiilor în care au fost copiate). Aceasta este de fapt și una dintre metodele cele mai des implementate de catre wormi[4] pentru a se propaga de la un calculator la altul.

- ***Win32. Worm. Downadup / Conflicker*** este celebrul worm care a infectat aproximativ 7 milioane de calculatoare în întreaga lume, folosindu-se de o vulnerabilitate Microsoft Windows pe RPC (MS08-67) care îi permitea să se copie și să se lanseze automat în toate calculatoarele existente într-o rețea. A fost primul worm care prezenta o metodă nouă de protecție a codului său, bazată pe ACL[5]-uri. Comportament de AV-Killer[6] (prin blocarea site-urilor celor mai populare produse antivirus, iar mai târziu la versiunile următoare și blocarea site-urilor pentru download-ul de removal tool[7]-uri).

- ***Trojan.Wimad.1.Gen*** este o detecție pe fișiere WMA (Windows Media Audio) sau WMV (Windows Media Video) care sunt special modificate pentru a rula diverse linkuri în momentul execuției lor.

- ***Exploit.SWF.Gen*** este o detecție generică pe exploituri de Adobe Flash. Detectează fișiere flash special modificate astfel încât la execuție să permită descărcarea și execuția unui executabil în sistem.

Din punct de vedere al rețelelor de boți[8], repartiția diferitelor tipuri de boți este mai uniformă pe anul 2009.

---

[3] Nu e cunoscut ca hijacker / injector

[4] Program care își copie codul în rețele de calculatoare, folosind diverse vulnerabilități existente în cadrul sistemului de operare.

[5] ACL reprezintă nivelele de securitate care se pot atribui unui obiect Windows (fișier, registru), prin care se stabilesc exact ce useri și ce permisiuni are fiecare asupra unui anumit obiect.

[6] Tehnica prin care un malware nu permite unui produs antivirus sa își facă update la fișierele de semnături.

[7] Removal Tool este un software creat de companiile AV care permite eliminarea unui anumit malware de pe un calculator.

Un bot este un malware, care rulează silent pe un calculator și menține un canal de comunicare cu un server. Rețelele de boți permit unui atacator să controleze în același timp mai multe calculatore. O astfel de rețea poate fi folosită pentru a ataca diferite servere (flooding / DoS), ca punct de plecare pentru spam-uri sau chiar ca o rețea de distribuție pentru alte tipuri de malware (Adware / RogueAV).

Tehnicile rootkit[9] devin un instrument utilizat frecvent de creatorii de rețele de boți (apar și mecanisme noi utilizate – cum ar fi patching-ul fișierelor sistemului de operare, sau chiar adăugarea de cod în afara partiției sistemului de operare).

Câteva măsuri de prevenire a fraudelor prin Internet în regim intern și trasfrontalier:

a. Frauda prin licitațiile online

- învățați cât se poate de bine cum funcționează licitațiile prin Internet, care sunt obligațiile dv. în calitate de cumpărător și care sunt obligațiile vânzătorului, toate acestea, înainte de a începe să licitați pentru un produs.
- examinați feedbackul vânzătorului oferit de alți cumpărători, dacă acesta are o istorie negativă de tranzacționare, nu faceți afaceri cu el.
- solicitați să știți ce metodă de plată preferă vânzătorul și unde solicită plata. Evitați serviciile de transfer rapid de bani indiferent de măsurile de protecție care vi se vor prezenta.
- întrebați vânzătorul despre modalitatea și timpul de livrare și despre orice condiții de garanție pentru produsul licitat.
- verificați dacă taxele de livrare sunt incluse în prețul produsului.
- nu furnizați Codul Numeric Personal, seria și numărul de buletin, pașaport sau permis de conducere întrucat vânzătorul nu are nevoie de aceste informații.

b. Frauda prin nelivrarea produselor

- asigurați-vă că achiziționați produsul dorit de la o persoană de încredere. În cazul licitațiilor online, verificați reputația vânzătorului ori de câte ori acest lucru este posibil.
- fiți precauți când tranzacționați cu persoane sau companii din afara țării.
- asigurați-vă că site-ul pe care tranzacționați folosește o conexiune securizată atunci când oferiți informații confidențiale de pe cardul dvs.

c. Frauda cu cărțile de credit

- nu oferiți niciodată informațiile de pe card dacă site-ul nu folosește o conexiune securizată și dacă reputația acestuia este îndoielnică.
- înainte de a utiliza site-ul, verificați ce software de securitate folosește pentru a vă asigura că datele dvs. sunt protejate.
- cardul dvs. este personal. Informațiile dumneavoastră sunt confidențiale. Nu oferiți aceste informații nimănui decât după ce v-ați asigurat de securitatea tranzacției.

d. Frauda cu investiții

- nu investiți în nici o afacere, bazându-vă pe aparențe. Nu investiți în nimic decât după ce sunteți absolut sigur și v-ați informat că afacerea este legitimă.
- informați-vă despre identitatea reală a celui care vă propune o afacere prin Internet și asigurați-vă că persoana este de încredere.
- REGULĂ: Dacă ceva sună prea frumos să fie adevărat, e foarte posibil să nu fie!

e. Furtul de identitate (PHISHING)

- nu accesați link-ul transmis în conținutul mesajelor e-mail primite de la adrese necunoscute (chiar dacă par surse de încredere). Practica a demonstrat numeroase atacuri de tip phishing în care e-mail-urile păreau să provină de la surse de încredere cum ar fi: banca la care aveți deschis un cont, organizația emitentă a cardului dvs. etc.
- verificați în browser numele site-ului, pentru a observa diferența față de site-ul original al instituției.
- Nu divulgați niciodată datele confidențiale despre conturile de card (număr de card, data expirării, codul PIN).

Concluzii: Fraudele informatice sunt realizate de specialiști care nu au un confort financiar pentru ei și familiile lor, dacă învățăm specialiștii în informatică să atingă confortul financiar necesar, atunci dorința de a câștiga bani din fraudă informatică se va diminua semnificativ.

Fiecare dintre noi are obligația să acorde multă atenție atunci când se fac diverse tranzacții pe internet. Nu este indicat ca datele personale (credit card, e-mail) să fie oferite cu ușurință.

Referințe:

[1] Ciureanu Sorin – "Sisteme de Operare", Ed. Printech, 2005

[2] Landau S. et al. – "Crypto Policy Perspectives", CACM, Aug 1994.

[3] Asociația "Vasile Pogor" Iași, Primul Simpozion de Prevenire și Combatere a Fraudelor Informatice; Editura D&T, 2010.