DOMENIUL CRIMINALITĂŢII INFORMATICE – SUBIECT DE PRESĂ

Prof.univ.dr. Emil STAN
Universitatea Hyperion

Abstract:

Concurrent with the development of IT we assisted to the growth of computer crime. In this paper we emphasize the current developments of a particular scourge, that of digital crime. The progress of information technology has occurred in parallel with changes in the methods used by criminals to break protections of digital computers. World states, including Romania, have had to develop specific legislation to prevent and combat cybercrime, to combat hacker activities, active subjects of such offenses. In the second part of the paper presents the activities of a famous journalist, specialist in digital crime investigation. The last part of the paper presents a methodology for developing a paper in this field, methodology that takes into account the specificities of this type of crime.

Keywords: investigation journalist, digital crime, hacker, methodology, legislation.

În lucrarea de față ne propunem să trecem în revistă evoluția unui flagel deosebit de actual, cel al infracționalității digitale. Dezvoltarea tehnologiei informatice a avut loc în paralel cu evoluția metodelor folosite de infractorii digitali pentru spargerea protecțiilor calculatoarelor. Statele lumii, inclusiv România, au trebuit să dezvolte o legislație specifică pentru prevenirea și combaterea criminalității informatice, pentru combaterea acțiunilor hackerilor, subiecții activi ai acestui tip de infracțiuni. În partea doua a lucrării se prezintă activitățile unui jurnalist renumit, specializat în investigarea infracțiunilor digitale. Ultima parte a lucrării prezintă o

metodologie de elaborare a unui articol în domeniu, metodologie care ține seama de specificul acestui tip de infracțiune.

1. Creșterea fără precedent a infracționalității digitale

Numai în SUA în 2014 mai mult de 3,2 milioane de oameni au depus plângeri de fraudă pe Internet sau de activități sub incidența legii combaterii infracționalității digitale, cu 16% mai mult decât un an în urmă, a anunțat rețeaua **Consumer Sentinel**, o ramură a *Comisiei Federale pentru Comerț*. Pierderile financiare au ajuns la 9,8 miliarde de dolari sau aproximativ 5.400 dolari pe o victimă care a raportat o pierdere financiară. Pierderi de 1 milion de dolari sau mai mult au fost raportate de 1557 de persoane.

Furtul de identitate a fost plângerea cea mai des întâlnită, reclamată de către 26% dintre victime. Frauda *card de credit* a fost cea mai comună formă de furt de identitate, aproximativ 20%. Cele mai multe victime ale fraudei informatice au declarat că escrocii le-au contactat inițial prin e-mail sau prin vizite la site-ul Web.

Potrivit firmei de cercetare și de securitate *Strategia Javelin*, în 2014, aproximativ 9,9 milioane de adulți din SUA au fost victime ale fraudelor de identitate, în creștere cu 22% față de anul precedent. Aceste fraude s-au soldat cu pierderi totale de 118 de miliarde de dolari. Cele mai multe incidente au fost rezultatul pierderii sau furtului de portofele, carnete de cecuri și cărți de credit, iar accesul on-line a reprezentat 11% din totalul raportărilor acestui tip de infracțiune.

Într-un articol recent se afirmă creșterea alarmantă a infecțiilor cu viruși și viermi informatici, precum și creșterea numărului atacurilor cibernetice. Organizația *F-Secure*, care monitorizează fenomenul începând cu anul 1991, a afirmat că doar în cursul anului 2014 frecvența acestor tipuri de atacuri a crescut cu 200% .

Afacerile suferă foarte mult datorită mulțimii atacurilor de securitate și a furtului de identitate, acestea producând pierderi mari. De asemenea, impactul financiar al acestor infracțiuni cibernetice este în creștere. Într-un alt articol, se afirmă că frauda on-line și escrocheriile de tip *phishing* au crescut pentru a avea un impact devastator pentru mai mult de 11,5 milioane de americani care cad victime schemelor de *phishing* și furtului de identitate on-line. Pe parcursul anului 2014 numărul victimelor a crescut cu 87% față de 2010, iar volumul furtului sumelor de bani a ajuns la 29,2 miliarde de dolari.

S-au înmulțit escrocheriile pe blog, a crescut pericolul de pretenții exagerate, al înșelătoriilor în cadrul licitațiilor on-line, al raportărilor false, al farselor web. Escrocheriile pe blog produc bani infractorilor. Asistăm la un număr tot mai mare de încercări de *phishing*, de falsuri. Crește, de asemenea, numărul impostorilor de pe web care se pretind a fi alte persoane decât cele din realitate. Este nevoie de efortul nostru comun, în anul 2015, pentru a lupta prin toate mijloacele împotriva celor care fură din cărțile de credit, împiedicându-i astfel să-și atingă, fără permisiunea noastră, propriile lor scopuri malefice. Nu trebuie lăsată garda jos împotriva celor care abuzează de noi în aceste moduri.

În general, în ciuda celor prezentate, web-ul și blogosfera sunt un loc foarte sigur pentru a desfășura în bune condiții comerțul on-line. Este însă nevoie de atenție și de luarea măsurilor de prevedere împotriva celor ce intenționează să se folosească ilicit de partea întunecată a forței Internetului.

2. Cazul jurnalistului Brian Krebs

Jurnalismul de investigație axat pe tema infracțiunilor digitale indică o înțelegere mai profundă a subiectului de către bandele criminale organizate cibernetice decât majoritatea polițiștilor ciberneticieni.

Brian Krebs este un astfel de jurnalist care a scris o mulțime de articole bine documentate pe această temă. Articolele au fost rezultatul unei munci asidue pe Internet, concentrându-se pe obținerea unor informații din site-urile de socializare, pe urmărirea activității pe net a șefilor grupărilor care se ocupă cu *criminalitatea cibernetică* din birourile lor. Aceste articole au servit, în marea lor majoritate, la prezentarea probelor penale detaliate în instanță de către organismele specializate ale poliției. Articolele elaborate de Krebs nu se rezumă numai la texte, ci sunt prezentate scheme, figuri, link-uri, bănci și conturi bancare, e-mailuri, conversații pe Facebook. Mai mult, investigațiile lui Brian se continuă prin interviuri luate unor infractori digitali care sunt considerați genii în **cyber space**. Unii dintre aceștia au fost arestați la câteva săptămâni în urma interviurilor.

Proiectele la care Brian a fost parte au împiedicat, cu siguranță, zeci de mii de oameni nevinovați de a deveni victime. Dedicarea lui Brian acestui subiect și dorința de a face bine au riscat propria liniște și bunăstare a jurnalistului. Amenințările mai mult sau mai puțin voalate pe care le-a primit l-au pus într-o permanentă alertă.

Brian și-a creat și un blog, *KrebsOnSecurity*, care a fost premiat cu 14 premii la concursurile de profil. Media cititorilor acestui blog este de 350.000 de vizitatori pe lună. El nu a făcut studii de specialitate în

Tehnologia Informațiilor. A ajuns cel mai bun în acest domeniu absolut din întâmplare. A început să scrie despre investigarea criminalității cibernetice în Washington Post, la sfârșitul anului 1995. Primele subiecte au fost legate de livrarea e-mail-urilor și, uneori, de securitatea calculatoarelor. A învățat cum să folosească Linux, apoi calculatorul său a fost lovit de *viermele Lion*. Această lecție pe care a primit-o din partea creatorilor de *malware* l-a determinat să-și crească interesul pentru securitatea calculatoarelor.

Astfel în 2002 a început să lucreze la **Washingtonpost.com**, unde s-a concentrat pe teme de securitate informatică. Editorii săi nu au apreciat întotdeauna ceea ce a postat pe acest site pentru că subiectele nu s-au concentrat tot timpul pe tipul de povești care într-un mod tradițional ar crește audiența. Mărturisește că de multe ori subiectele pe care le-a lansat - și care au fost respinse de la continuare de editori - au ajuns câteva săptămâni mai târziu, în alte ziare, cum ar fi Wall Street Journal. Astfel editorii au început să aprecieze treptat valoarea acestor subiecte. Drept urmare a fost încurajat să creeze primul său blog, SecurityFix. În felul acesta a putut să scrie mai mult și mai repede decât ar fi putut să o fi făcut în presa scrisă.

În 2009, **washingtonpost.com** a fuzionat cu ziarul tipărit. Dorind să continue să scrie despre subiectele legate de criminalitatea informatică a început un blog nou, KrebsOnSecurity, la sfârșitul anului 2009. Astfel a părăsit un ziar foarte respectat pentru a se consacra blogosferei.

În felul acesta a căpătat libertatea de a scrie despre subiectele cyber-criminalității. Blog-ul îi dă timp să se dedice unui anumit subiect pe care să-l dezvolte mai mult, abordând și toate subiectele conexe. Temele nu mai sunt alese de altcineva. Poate să-și gestioneze timpul și resursele asupra subiectelor care i se par interesante.

Un astfel de subiect a fost legat de *criminalitatea informatică rusă*, iar pentru investigarea acesteia a observat cu atenție *Russian Business Network*. A învățat limba rusă și s-a mutat în Rusia. A putut realiza că în fenomenul criminalității cibernetice majore sunt implicați sute de oameni, mulți dintre ei ruși, dar și mulți din fostele republici sovietice. Câteva sute de oameni produc **malware**, phishing, spamming și așa mai departe. Există o mulțime de executanți, dar cei care sunt liantul pentru comunitatea infracțională digitală rusă alcătuiesc un grup mult mai mic, mai mult de elită.

Nu a spus nimănui că are de gând să se deplaseze în Rusia. Desigur, acest fapt i-a surprins pe oamenii pe care i-a văzut acolo. Dacă ar fi știut că vine, poate că nu s-ar fi întâlnit cu acesta. Surpriza este un instrument frumos care poate da rezultate. Desigur, atunci când a ajuns prima oară în Rusia, la Sankt-Petersburg au fost momente de derută în rândul infractorilor

digitali. S-a dat o alertă pe Google pentru numele lui Krebs, precum și pe diverse site-uri de criminalitate cibernetică din Rusia. Pe unele blog-uri rusești au existat postări care spuneau tuturor că jurnalistul american a ajuns acolo, indicându-se și la ce hotel stătea.

Krebs a realizat în urma a aproape 20 de ani de studiu al infracționalității digitale că atât timp cât nivelul de corupție este atât cât este, va fi dificilă eradicarea acestui flagel. De exemplu, în acest caz, era clar că persoanele pe care acesta le intervievase erau implicate în infracționalitatea digitală majoră, prin urmare erau pe cale de a fi arestate. Totuși, autoritățile însărcinate cu aplicarea legii nu le-au arestat imediat. Infractorii au avut timp să se strecoare afară din țară. Urmărirea și dovedirea criminalității cibernetice-financiar este dificilă. Este mult mai ușor pentru autorități să condamne, de exemplu, pornografia infantilă.

Site-ul jurnalistului suferă foarte multe atacuri de tipul DoS (denial-of-service). Pentru a se apăra de aceste atacuri, Krebs dispune de un puternic software anti-DoS care îi este de mare ajutor.

3. Pași necesari pentru elaborarea unui articol despre criminalitatea informatică

1. Aveți misiunea de a scrie un articol despre o infracțiune digitală. Puteți avea, de asemenea, unele întrebări inițiale cu răspunsuri deja cunoscute, cum ar fi "*când*?" sau "*unde*?" Dar acum este esențial de a face unele săpături inițiale pentru a afla *cine*? *de ce*? și *cum*? Găsiți sursele. Internetul este plin de informații pe această temă. Puteți consulta site-urile poliției și FBI-ului, site-uri universitare și alte site-uri, cum ar fi cele ale producătorilor de software de securitate pentru mai multe informații. Ați putea dori, de asemenea, să utilizați cărțile elaborate de experți în *securitate informatică*. Uneori se impune intervievarea unor oficiali ai poliției cu ajutorul informațiile de contact de pe site-urile respective.

2. Faceți o *schiță* a articolului. Descompuneți problematica pe diferite domenii și subiecte pe care doriți să le abordați în articol. În timp ce desfășurați activități de cercetare, veți obține o mai bună înțelegere a modului în care piesele se potrivesc împreună și ce domenii se armonizează și pot fi abordate împreună. Scrieți note și *piese cheie din informații*, imediat ce le găsiți. Acest lucru vă va ajuta să vă organizați gândurile, iar articolul va curge în mod rațional. Reveniți apoi și completați secțiunile cu gânduri mai sofisticate și mai complexe, identificând noi probe informatice din *suporții de informații* sau de pe Internet. Puneți informațiile împreună într-un mod util, coerent asigurând însă și un anumit grad de suspans, atunci

când este posibil, pentru a face articolul mai interesant. Asigurați-vă, pentru a face note de subsol, că ați efectuat documentarea corectă. În cazul în care informațiile provin din alte articole evitați astfel eventualele *acuzații de plagiat*.

3. Odată ce informația a fost descoperită și ați intervievat *cel puțin trei surse diferite* despre această infracțiune specială (orice reporter ar trebui să facă acest lucru pentru fiecare poveste pe care o scrie), e timpul să vă așezați în fața calculatorului cu toate elementele obținute, asigurându-vă că ați pus toate lucrurile importante în partea de sus, iar jos, lucrurile mici, mai puțin importante.

4. Atrageți cititorul în povestea dumneavoastră, probabil prin prezentarea câtorva detalii de setare interesante (de exemplu, "în timp ce întregul oraș s-a adunat pentru dezvelirea noului monument din fața primăriei vineri după-amiază, o activitate suspectă avea loc în Internet."). În cazul de față, *infracțiunea informatică* prin care s-au scos bani din bancomate s-a desfășurat vineri după-amiaza, în timp ce foarte multă lume participa la un eveniment organizat în fața primăriei, astfel că strada pe care se afla bancomatul era pustie.

5. Analiza informațiilor deținute conduce la nevoia unor precizări pentru cititori, răspunsuri la întrebări de genul *care*?, *ce*?, *unde exact*? și *de ce*? Ar trebui efectuate și interviuri cu un ofițer de poliție sau detectiv, cu martori, precum și, în funcție de infracțiunea digitală, cu oricine altcineva care ar putea să facă lumină asupra situației. Dacă este vorba de încasarea unor bani de la bancă pentru o **licitație online trucată** și principalul suspect este băiatul de alături, care stă toată ziua în Internet-Cafe și se pregătește să participe la un colegiu informatic, dar nu există martori privind desfășurarea infracțiunii, se simte nevoia unor discuții cu vecinii care-l cunosc pe băiat. Se adună impresiile, iar în articol se pot introduce citate din aceste interviuri pentru a sprijini faptele și a prezenta perspective diferite. Cu cât vă infiltrați mai adânc în înțelegerea infracțiunii, iar articolul începe să se contureze, se recomandă *abținerea de la introducerea propriei opinii în articol*. Sarcina jurnalistului este de a prezenta publicului fapte analizate la rece și nu părerea acestuia privitoare la incident.

6. Asigurați-vă că faptele cele mai concrete și mai interesante sunt în prima parte a articolului, iar textul mai puțin interesant în continuare. Acest lucru va permite editorului să reducă rapid de jos în sus, în cazul constrângerilor de spațiu, acesta știind că nu va tăia din elementele pertinente. De asemenea, editorul se asigură că cititorul va primi esența poveștii în primul calup de paragrafe și nu va fi nevoie de a continua lectura eventual pe o altă pagină pentru a afla ce s-a întâmplat.

7. În cele din urmă, înainte de depunerea articolului editorului dvs., verificați toate faptele și citatele cu sursele. Odată cu depunerea articolului se oferă și o listă cu sursele și informațiile de contact, împreună cu orice alte elemente ce pot fi menționate că au stat la baza articolului. Multe publicații efectuează o nouă verificare a surselor și vor avea nevoie de cel puțin de această listă. Unele ziare și reviste solicită, de asemenea, o versiune adnotată a articolului, împreună cu note de interviu. Dacă interviurile sunt realizate prin telefon sau înregistrate, este nevoie și de transcrierea acestora și oferirea acestor transcrieri editorului. Îmbunătățiți permanent abilitățile dumneavoastră de scriere. Pentru aceasta este necesar ca zilnic să scrieți timp de cel puțin o oră, pe calculator, un text. Acest lucru vă va ajuta să vă găsiți mai ușor cuvintele potrivite, să vă măriți viteza de scriere la calculator, să vă exprimați corect. Dacă este necesar, explorați mai multe resurse oferite pe Internet și faceți trimiterile necesare pentru a ajuta cu lucrări de cercetare pe cei ce doresc să aprofundeze subiectul. Faptele trebuie să fie prezentate într-un mod care este ușor de înțeles de către public pentru a avea impactul dorit.

Bibliografie

1. Emil STAN, *Războiul Hackerilor*, Editura Kulusis, București, 2009
2. Emil Stan, Infowar, *Editura Triumf*, București, 2010
3. Petru Ignat, Emil Stan, *Proiectarea și realizarea produsului jurnalistic*, Editura Victor, București, 2011
4. www.krebsonsecurity.com
www.washingtonpost.com