DOI: 10.5937/vojdelo1703099D

KRAĐA IDENTITETA – OBLICI, KARAKTERISTIKE I RASPROSTRANJENOST

Anđelija Đukić
Univerzitet u Beogradu, Fakultet bezbednosti

U radu se razmatraju osnovni pojavni oblici kompjuterskog kriminala sa težištem na krađi identiteta kao posebnom obliku pri kojem se vrši nelegalno pribavljanje poverljivih ličnih podataka radi izvršenja novih krivičnih dela. Prikazani su osnovni metodi i tehnike krađe podataka o ličnosti od krajnjih korisnika interneta, sa ličnih računara i iz velikih baza podataka i upotreba ukradenih podataka za izvršenje krivičnih dela. Na osnovu dostupnih podataka prikazane su tendencije porasta broja i oblika visokotehnološkog kriminala i krađe identiteta kod nas i u svetu. Sagledan je mogući razvoj novih i usavršavanje postojećih metoda i tehnika za krađu identiteta i posledice njihovog korišćenja za izvršenje krivičnih dela.

Ključne reči: *internet, visokotehnološki kriminal, baze podataka, krađa identiteta, pojavni oblici, karakteristike*

Uvod

Veoma brz razvoj informacionih i komunikacionih tehnologija (IKT) i njihova primena postali su neizbežan faktor u oblikovanju društvenog života koji pruža mogućnost novih načina komuniciranja, informisanja, obrazovanja, rada i zabave. Rast i razvoj globalnih računarskih mreža doprinosi i naglom narastanju broja zloupotreba IKT kao što su: narušavanje poverljivosti informacija, ometanje njihove funkcionalnosti kroz poremećaje operacija među njima, uzurpiranje i krađa intelektualnih dobara, razne vrste drugih krađa i prevara, kao i druge mnogobrojne zloupotrebe koje se razlikuju po motivima, ciljevima, metodima i načinima ostvarivanja. Visokotehnološki (VT, sajber, kompjuterski) kriminal je veoma složen oblik kriminala; poseduje veliku dinamičnost, stalno se širi i razvija nove oblike, nema teritorijalnih ograničenja i praktično ne poznaje državne granice ili geografska ograničenja. Globalna mreža internet ima velike pogodnosti za primenu i širenje kriminala, pruža mogućnost lakog udruživanja kriminalaca sa različitih prostora u svetu i za njih predstavlja dobro skrovište. Zbog svoje specifičnosti delovanja na daljinu i velike mogućnosti prikrivanja počinilaca, ovaj kriminal se otežano otkriva i dokazuje, tako da se u međunarodnim okvirima preduzimaju opsežne mere za njegovo sprečavanje, otkrivanje i sankcionisanje.

Visokotehnološki kriminal je relativno novi oblik kriminalnog ponašanja i pri njegovom određenju može se naći veliki broj različitih definicija, ali sve one u velikom obimu imaju zajedničke elemente, pre svega da je u vršenju kriminalne radnje korišćena tehnika visoke tehnologije i da je pri tome naneta šteta žrtvama kriminalne radnje. Obim kriminalnih

radnji je veoma širok: od nedozvoljenog umnožavanja autorskih dela, krađa i pronevera milionskih novčanih i drugih vrednosti, sabotaža, vandalizma i terorizma, pa do izvršenja ubistava. Opšteprihvaćen je stav da će u budućnosti VT kriminal, pored širenja na račun običnog kriminala, stalno razvijati svoje oblike i tehnike realizacije.

Informatička (softver) i tehnička (prostor i hardver) zaštita stalno se unapređuju u suprotstavljanju kriminalcima, ali u njihovoj sferi interesovanja sve češće je prisutan pristup željenim podacima preko zaposlenih lica, bilo da su u pitanju insajderi u firmama ili slaba obučenost, nepažnja ili nemar zaposlenih. Nivo profesionalne osposobljenosti i primenjivani metodi kriminalaca u stalnom su razvoju i usavršavanju, što čini realnom opasnost od velikih materijalnih i drugih vrsta šteta koje mogu da pretrpe žrtve VT kriminala; zato je od velikog značaja zaštita podataka koji su, ili mogu da budu, meta napada kriminalaca.

Ovaj rad ima za cilj da pokaže mesto krađe identiteta u spektru raznih kriminalnih radnji koje se svrstavaju u VT kriminal, neke njene karakteristike, pojavne oblike i rasprostranjenost. Pri tome će se krađa identiteta razmatrati i prema lokaciji smeštaja i čuvanja podataka i izvršenja krađe; to su prvenstveno lični računari i računarski sistemi i mreže, a u novije vreme i drugi mobilni IKT uređaji povezani sa globalnom računarskom mrežom.

Donošenjem odgovarajućih zakona kojima se bliže uređuje oblast informacione bezbednosti i otkrivanje, krivično gonjenje i suđenje za krivična dela VT kriminala, a posebno Zakona o informacionoj bezbednosti[1], postavljeni su osnovi za veću bezbednost podataka o ličnosti, a time i smanjenje opasnosti od krađe identiteta. Uspostavljanje celovitog sistema informacione bezbednosti u Srbiji i njegovo funkcionisanje preduslov su bezbednijeg funkcionisanja računarskih sistema i mreža, a time i smanjenja rizika od otuđenja podataka o ličnosti, odnosno krađe identiteta.

Krađa identiteta

Pojam krađe povezane sa IKT, pored krađe koja se izvodi tako da se otuđuju IKT uređaji i njihove komponente, podrazumeva krađu raznovrsne robe, krađu računarskih usluga, krađu podataka, krađu kodova, lozinki i identifikacionih brojeva i krađu identiteta.[2] Mrežno okruženje i internet pružaju velike mogućnosti za krađu poslovnih i drugih tajni, softvera i autorskih dela, ali i za krađu ličnih tajni i njihovo korišćenje za krađu novca i druge napade na ličnosti. U porastu je broj krađa podataka sa ličnih računara ili mobilnih uređaja, kao i iz velikih baza podataka koje raspolažu milionskim zapisima o ličnostima, a sve radi finansijskih zloupotreba od strane kradljivaca, radi dalje prodaje na crnom tržištu ili ucenjivanja kompanija i organizacija koje čuvaju podatke.

Zlonamerno ili iz koristoljublja ukradeni identiteti ličnosti mogu se iskoristiti za široki spektar kriminalnih radnji, pojedinačno ili češće njihovim kombinovanjem, od kojih su osnovne: krađe, prevare, falsifikovanje i narušavanje privatnosti, a s tim u vezi su i kriminalne radnje pronevere, iznude, uznemiravanja, ucene, dečija pornografija i dr.

Iako postoje različite definicije krađe identiteta kao oblika VT kriminala, svi bitni elementi obuhvaćeni su sledećim određenjem: „Krađa identiteta (*identity theft*) je forma kri-

[1] NS RS, „Zakon o informacionoj bezbednosti", *Sl glasnik RS*, br.6/2016.

[2] Slobodan R. Petrović, *Kompjuterski kriminal* (Beograd: Vojnoizdavački zavod, 2004), 133.

minala u kojem neko koristi tuđi identitet da bi izvršio kriminalnu radnju."[3]To je poseban oblik VT kriminala koji objedinjava nelegalno pribavljanje poverljivih ličnih podataka za jedno ili više lica i njihovo korišćenje za izvršenje novih krivičnih dela. Nelegalno pribavljanje podataka o ličnosti obavlja se bez znanja osobe koja je žrtva, a pri tome se prisvaja njeno ime i drugi lični podaci.

Pod opštim pojmom krađe identiteta mogu se podrazumevati različiti modeli i pojavni oblici krađe podataka o ličnosti i veliki broj metoda i postupaka njihove upotrebe pri izvršenju novih kriminalnih radnji, različiti profili žrtava, sadržaji i vrednosti šteta koje se nanose žrtvama i druge specifičnosti. Čin krađe podataka o ličnosti obično ima svoj krajnji cilj koji se postiže izvršenjem novog krivičnog dela, čije posledice mogu da budu materijalne ili nematerijalne prirode. Krajnji ciljevi krađe identiteta, pored finansijskih ili političkih, mogu da budu ucene, terorizam i slično. Zato se krađa identiteta može posmatrati u užem i širem smislu:

– u užem smislu to je nelegalan postupak pribavljanja željenih podataka o jednoj ili više ličnosti;

– u širem smislu, pored pribavljanja podataka o ličnostima, krađa identiteta obuhvata njihovu upotrebu ili prodaju na crnom tržištu, ustupanje drugim licima i dalje korišćenje za izvršenje drugih kriminalnih radnji[4].

Identitet se krade korišćenjem tuđe lične karte, vozačke dozvole, JMBG ili sličnih personalnih podataka kojima se može izvršiti krivično delo na štetu ili u ime žrtve. To stvara i dodatne probleme za žrtvu, čak i onda kada je izvršilac uhvaćen, jer može da joj naruši ugled, a u otklanjanju posledica žrtva troši mnogo vremena i novca. Ova krađa može se obaviti krađom novčanika ili torbice sa dokumentima, korišćenjem tehničkih sredstava za pojedinačne krađe identiteta, ali i krađom podataka sa računara ili mobilnih uređaja, sa i bez korišćenja mrežnog okruženja.

Ranije je često, kao zamena za izraz „krađa identiteta", u upotrebi bio izraz „socijalni inženjering", koji je u sadržajnom smislu širi pojam i podrazumeva manipulisanje ljudima ubeđivanjem i lažnim predstavljanjem radi pribavljanja željenih informacija, pri čemu ne moraju da se koriste tehnička sredstva. Iako izraz nije adekvatan postupcima koje opisuje, osobe koje se bave bezbednošću računara pod socijalnim inženjeringom podrazumevaju tehnike ubeđivanja i obmanjivanja radi dobijanja pristupa informacionom sistemu.[5] Za komunikaciju se obično koriste kompjuter ili telefon, kroz forme e-pošte, propagandnih poruka ili neke od bezbroj drugih mogućnosti, kako bi se izazvala reakcija ljudi i omogućio pristup željenim informacijama. Razvojem i stalnim usavršavanjem zlonamernog softvera, metoda i tehnika nasilnih upada u velike baze podataka o ličnosti i intenziviranje neprekidne borbe između kriminalaca i ljudi koji se bave bezbednošću IKT sistema, ova dva pojma se sve više razdvajaju i među njima nema više jakih veza.

[3] Isto, 141.

[4] Cifas, „Identity Fraud", https://www.cifas.org.uk/identity_fraud:

Slična razgraničenja krađe identiteta mogu se naći i kod drugih izvora, tako da npr. *CIFAS*, kompanija iz V. Britanije koja se bavi zaštitom firmi, dobrotvornih ustanova, javnih organa i ustanova i pojedinaca od finansijskog kriminala, definiše „zločin (kriminal) identiteta" kao novi pojavni oblik kriminala gde izvršioci koriste tuđe lične podatke, a kriminal identiteta dele na *krađu identiteta (identity theft)* kada su ukradeni lični podaci i na *identitet prevaru (identity fraud)* kada su ti podaci upotrebljeni za kriminalne aktivnosti.

[5] Stjuart Meklur, Džoel Šambri i Džordž Kurtc, *Hakerske tajne: zaštita mrežnih sistema*, prevod Dejan Smiljanić i Milenko Šućur (Beograd: Mikro knjiga, 2006), 594.

Podaci o ličnosti[6], kao meta kriminalaca u postupku krađe identiteta, nalaze se kod svakog lica pojedinačno, ali i u mnogobrojnim bazama podataka kojima raspolažu državni organi, osiguravajuća društva, bezbednosne institucije, korporacije i drugi sistemi. Značaj zaštite podataka o ličnosti je u tome da ona predstavlja garanciju prava na privatnost kao jednog od osnovnih ljudskih prava. Zloupotreba podataka o ličnosti može da ima dugotrajne i veoma štetne posledice po žrtvu, a jedna od njih je i krađa identiteta sa pratećim negativnostima po žrtvu. Nedozvoljenim pristupom u velike baze podataka mogu se pribaviti podaci o milionima lica, čime se može izazvati ogromna šteta.[7]

Načini i tehnike krađe identiteta

Pojavni oblici krađe identiteta, posmatrani u užem smislu i prema lokaciji smeštaja informacija o ličnosti i korišćenim sredstvima i tehnikama za njihovo nelegalno pribavljanje, mogu se razvrstati na tri široke grupe:

– krađa identiteta klasičnim metodima i izvan IKT sistema i mreža;
– krađa identiteta sa ličnih računara i mobilnih uređaja u mrežnom okruženju;
– krađa identiteta iz IKT sistema i mreža.

A) Krađa identiteta klasičnim metodima

Krađe identiteta klasičnim metodima ne isključuju upotrebu različitih tehničkih sredstava, ali je karakteristično da se do podataka ne dolazi putem računarskog sistema i računarske mreže. Pri korišćenju ovako prikupljenih podataka i neposrednog odnosa kriminalca sa žrtvom ili subjektom prevare, veći je rizik da kriminalac bude otkriven. Prema ciljevima učinilaca krađe identiteta i ostvarenim negativnim efektima na žrtvu, jedna od mogućih podela je:

– *finansijska krađa identiteta,* koja predstavlja korišćenje tuđih ličnih podataka radi finansijske koristi preko podizanja kredita, odobravanja kreditnih kartica ili podizanje novca sa bankovnih računa. Neke od primenjivanih tehnika su: skeniranje bankovnih kartica (kamere, „skimeri" ili „skederi" koji se ugrađuju na bankomate), falsifikovanje dokumenata, kloniranje kartica i drugo, pri čemu se podaci o ličnosti koriste pojedinačno;

– *medicinska krađa identiteta,* koja je po žrtvu posebno opasan oblik krađe identiteta, jer može da ugrozi život pokradene osobe zbog promena podataka u zdravstvenim dokumentima žrtve. Koriste je lica koja nemaju zdravstveno osiguranje ili žele dodatne beneficije (korišćenje posebnih zdravstvenih institucija, specijalni tretman i slično). Ovaj oblik

[6] Podatke o ličnosti i njihovu upotrebu i zaštitu u Srbiji definiše „Zakon o zaštiti podataka o ličnosti", *Sl. glasnik RS*, br.97/2008,104/2009, 68/2012 i 107/2012.

[7] Ukrali 130 miliona kreditnih kartica, *Politika*, 18.08.2009. http://www.politika.rs/sr/clanak/100340/Ukrali-130-miliona-kreditnih-kartica:

U SAD je u periodu od oktobra 2006. do maja 2008. tročlana hakerska grupa upadom u baze podataka vlasnika platnih i kreditnih kartica u tri velike maloprodajne kompanije ukrala oko 130 miliona brojeva kartica radi dalje prodaje na veliko preko interneta, a neki od njih korišćeni su za podizanje novca, za neovlašćene kupovine ili štampanje falsifikovanih kartica sa originalnim brojevima i kodovima. To predstavlja najveću krađu podataka o ličnosti koja je prijavljena i poznata široj javnosti do 2010.

krađe je posebno zastupljen u zemljama sa velikim brojem ilegalnih imigranata, a njegove posledice se teško ispravljaju;

– *krivična krađa identiteta*, koja podrazumeva da se pri izvršenju nekog krivičnog dela koriste tuđi dokumenti, što za žrtvu može da ima velike negativne posledice, jer je kasnije teško dokazati da žrtva nije učinila navedeno krivično delo;

– *krađa JMBG-a* koji sadrži bitne podatke o ličnosti (datum rođenja, pol, republiku i područje rođenja u SFRJ ili prebivalište) može za žrtvu da predstavlja velike neprijatnosti zbog njegove zloupotrebe pri prevarama državnih, poreskih i drugih organa, zdravstvenih institucija, podizanja kredita ili korišćenjem beneficija koje ima žrtva. Jedinstveni matični broj građana može se iskoristiti za falsifikovanje dokumenata žrtve ili pribavljanje duplikata dokumenata od škola, fakulteta ili poslovnih organizacija. Ukradeni JMBG može da bude posebno koristan za nekoga ko dobro poznaje žrtvu i raspolaže i drugim podacima o njoj (rođačke, prijateljske ili poznaničke krađe);

– *sintetička krađa identiteta* podrazumeva spajanje podataka više lica i stvaranje novog identiteta. Novi identitet ne pripada jednom licu, ali sva lica čiji su podaci ukradeni i ugrađeni u novi identitet mogu imati negativne posledice pri njegovom korišćenju;

– *poslovna krađa identiteta* koristi se za dobijanje kredita ili sticanje drugih beneficija u poslovnom svetu korišćenjem podataka o vlasnicima firmi.

Preduzimanje mera za zaštitu ličnih podataka od strane korisnika, kako bi se sprečile navedene krađe identiteta, ne samo da je potrebno već je i obavezno. Međutim, bezbednost informacija o pojedinoj ličnosti ne zavisi samo od nje same, jer se ti i mnogi drugi podaci nalaze u mnogobrojnim bazama podataka kod državnih organa, banaka, preduzeća, trgovinskih kompanija i drugih, uglavnom izvan kontrole građana.

B) Krađa identiteta sa ličnih računara i mobilnih uređaja

Povećanju rizika u primeni IKT veliki doprinos daje eksplozivan razvoj i rast globalnih računarskih mreža u koje je uključeno oko tri milijarde korisnika širom Zemlje, sa ogromnim brojem tehničkih sistema, veza, sadržaja i mogućnosti.

Upotreba interneta u državama EU beleži rast u svim sferama života, što pokazuju istraživanja koja se sprovode za potrebe Evropske komisije[8] i po metodologiji Agencije za statistiku EU (Eurostat). Rezultati istraživanja za zemlje članice EU i Uniju u celini za 2014. godinu zasnivaju se na ispitivanju pojedinaca na uzorku od blizu 28 hiljada ispitanika u svih 28 država članica EU. S obzirom na velike razlike među državama u stepenu ekonomskog razvoja i različitosti u kulturnim, obrazovnim i drugim oblastima života, korišćenje računara i interneta po državama je veoma raznoliko. Tako npr. u Švedskoj, Holandiji i Danskoj *svakog dana* internet koristi oko 90% ispitanika, dok u Rumuniji, Portugalu, Grčkoj i Bugarskoj internet koristi *povremeno* oko 55% ispitanika, a ostali ispitanici mu nikada nisu pristupili . Na nivou svih država EU internet koristi oko 76% ispitanika (od toga 63% svakog dana), dok 24% ispitanika nikad nije koristilo ili nema pristup internetu.

[8] European Commision, „Ciber security report 2014", *Special Eurobarometer 423*, februar 2015, 4-18, http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf.

Upotreba IKT i interneta u Srbiji takođe je u stalnom porastu na nivou državnih institucija, privrede, domaćinstava i pojedinaca. Na teritoriji Republike Srbije[9] (bez AP KiM) u 2016. godini 99,8% preduzeća koristilo je računar u svom poslovanju i ima internet priključak, a preko 80% poseduje i svoju veb stranicu. Bar jedan računar poseduje 65,8% domaćinstava, a 64,7% domaćinstava poseduje internet priključak kod kuće.

Najčešća veza sa internetom su mobilni telefoni (76,5%) i personalni računari (72%), što je novina u odnosu na prethodni period kada je veza putem računara bila primarna. Preko 3.610.000 lica (67,1%) koristilo je računar i internet u poslednja tri meseca, dok 27,2% lica nikad nije koristilo računar. Od ukupnog broja korisnika internet koristi svakog ili skoro svakog dana preko 3.070.000 lica (85% internet populacije), a najčešće se čitaju onlajn novine ili časopisi (77,4%), traže informacije o robi i uslugama (71,3%) i učešće u društvenim mrežama (68,7%), za razliku od 2015. godine kada je primarno bilo korišćenje interneta za učešće u društvenim mrežama (75,6% internet populacije). Preko 1.510.000 građana (oko 42% internet populacije) koristi internet za pristup organima javne uprave, preko 1.450.000 lica (38,3% internet populacije) kupovalo je robu/usluge putem interneta u poslednjih godinu dana, a internet bankarstvo koristi oko 20% internet populacije ili oko 760.000 građana Srbije.

Na osnovu rezultata u istom istraživanju[10] može se zaključiti da se veliki broj pojedinaca koji su korisnici interneta ponaša veoma neoprezno (ili bolje: veoma neodgovorno) prema ličnim podacima koji mogu da budu predmet krađe identiteta: tokom poslednjih dvanaest meseci samo 27,7% internet populacije nije davalo (ostavljalo) nikakve lične podatke putem interneta, dok je 56,7% lica činilo dostupnim lične podatke (ime, datum rođenja, podaci sa lične karte i dr), 53,6% lica je davalo kontakt podatke (adresa, broj telefona, imejl i sl), a čak 10,4% lica je činilo dostupnim podatke u vezi sa plaćanjima (broj kreditne ili debitne kartice ili broj bankovnog računa).

Radi upoređenja stanja korišćenja interneta u Srbiji i u državama EU, prema podacima za 2014. godinu, a kako je primenjena ista (Eurostat) metodologija (broj ispitanika u Srbiji bio je 2.400 pojedinaca starosti između 16 i 74 godine), izabrane su države sa najvećim (Švedska) i najmanjim (Rumunija) korišćenjem interneta i nama susedne države Mađarska i Hrvatska. Izabrani parametri prikaza su:

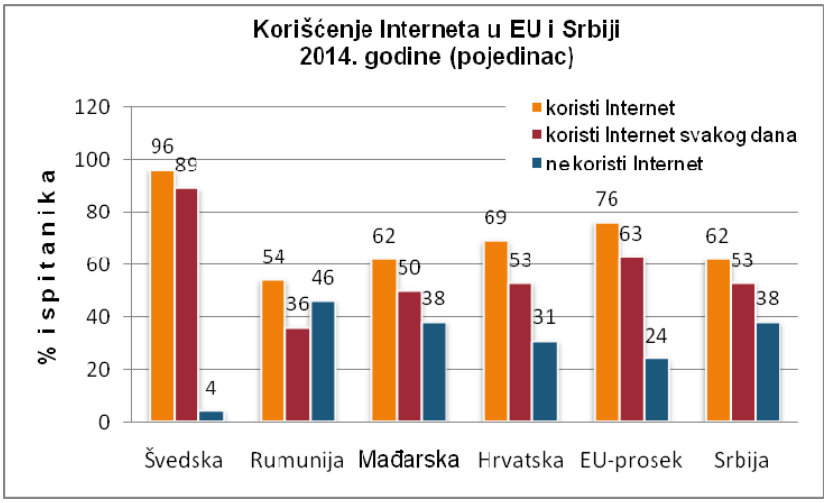
– koristi internet u poslednja 3 meseca,

– svakodnevno ili skoro svakodnevno koristi internet.

Iz prikaza na slici 1 može se zaključiti da je stanje u Srbiji po pitanju upotrebe interneta još uvek na niskom nivou, posebno ako se zna da se on koristi prevashodno za čitanje onlajn novina, a u manjem obimu za obavljanje drugih poslova.

[9] RSZ. *Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji, 2016*, (2016), 12-29. http://webrzs.stat.gov.rs/WebSite/repository/documents/00/02/25/89/ICT2016s.pdf

[10] Isto, 32.



Slika 1 – *Korišćenje interneta u Srbiji, odabranim državama EU i prosečno u EU u 2014. godini*[11]

Internet kao globalna mreža pruža mnogo pogodnosti, ali su zato i svi učesnici i akteri u tom sistemu ujedno i potencijalne mete napada radi krađe ličnih podataka, novca sa računa ili poslovnih informacija.

Za *krađu identiteta sa ličnih računara* koji su u sistemu interneta razvijen je veliki broj metoda i njihovo precizno razdvajanje praktično je nemoguće, ali se mogu izdvojiti dva osnovna:

– fišing (*phishing*) sa podvrstama višing (*vishing*) i smišing (*smishing*), i

– primena malvera (*malware*), sa podvrstom farming (*pharming*).

Zbog opasnosti i mogućih šteta, kao i načina i metoda postupanja kriminalaca, posebno se mora razmatrati primena familije malicioznog softvera pod nazivom ransomver (*ransomware*), pri čemu se zlonamerni softver instalira na računar žrtve, a njegovim aktiviranjem onemogućava se normalan rad računara i žrtva se ucenjuje da otkupi šifru kojom će eliminisati negativan uticaj instaliranog malvera. Sa aspekta kriminalaca i prema ostvarenoj koristi postupak je još delotvorniji ako se primenjuje na velike IKT sisteme radi ucene.

Svaki od ovih načina (metoda) ima svoje prepoznatljive karakteristike, ali im je zajednički cilj: prisvajanje tuđeg novca ili ispoljavanje drugog negativnog uticaja na žrtvu (ucene, kompromitovanje i drugo).

Fišing (pecanje) jeste pojam koji se odnosi na prevare radi dobijanja zahtevanih podataka od lica kome su ti podaci poznati. Pri tome se obično koristi faktor hitnosti na koji žrtva treba da reaguje, a prvi korak je slanje zlonamerne e-pošte kao mamca. Tipična fišing poruka izgleda kao poruka poslata od poznate institucije (banke, pošte, trgovinske

[11] Izvori podataka: European Commision, „Ciber security report 2014" (videti fusnotu 9); RSZ. Upotreba *informaciono-komunikacionih tehnologija u Republici Srbiji, 2014*. (2014), 19. http://webrzs .stat.gov.rs/WebSite/repository/documents/00/01/50/47/ICT2014s.pdf.

kompanije, penzionog fonda i slično). Poruka sadrži sakrivenu vezu sa ilegalnim sajtom na kojem će se slati tražene informacije ili je poruka prenosnik zloćudnog softvera koji će biti instaliran na računaru žrtve i postepeno prikupljati tražene podatke. Fišing je metod koji šalje jednu poruku hiljadama primalaca[12], od kojih će većina aktivirati poruku, a mnogi i dati tražene podatke. *Višing* i *smišing* su verzije tehnike pecanja. U metodu višing umesto e-poruke koristi se telefonski razgovor i tehnike socijalnog inženjeringa (manipulisanje i dovođenje žrtve u zabludu) kako bi se žrtva navela da oda svoje podatke finansijske prirode. U tehnici smišing koristi se mobilni telefon i tekstualne poruke umesto e-pošte, sa istom opasnošću i posledicama kao i u metodu fišing.

Malveri (maliciozni softver) koji se primenjuju u fazi prikupljanja i zloupotrebe podataka, pored fišinga, najrasprostranjeniji su način krađe identiteta. Malveri ili maliciozni (zlonamerni) softver su programi koji su ubačeni u računar žrtve bez njenog znanja sa ciljem da ometaju rad računara ili prikupljaju tražene podatke. Prema načinu rada zlonamernog softvera to mogu biti: virusi, crvi, trojanci, špijunski softver, farming i druge vrste, koje se međusobno prepliću i ne isključuju, a zajedničko im je da nanose štetu žrtvi (onemogućavaju normalan rad računara, špijuniraju rad ili preuzimaju podatke, kao i kontrolu računara promenom ovlašćenja za rad).

Za nedozvoljenu finansijsku transakciju i prevaru, korišćenjem malvera, proces se može prikazati u tri koraka[13]:

1. Zaraza računara žrtve. Distribucija malicioznog softvera na računar žrtve može se obaviti nekom lažiranom i od strane žrtve prihvatljivom e-porukom, oglašavanjem, korišćenjem bezbednosne ranjivosti u pretraživačima ili drugom korisničkom softveru i slično, gde se učitava kod koji vodi do malvera.

2. Prikupljanje podataka bitnih za novčanu transakciju (kredencijala) obavlja se: snimanjem ekrana ili tastature, praćenjem kucanja na tastaturi, praćenjem vremena prijavljivanja prema banci, preusmeravanjem internet pretraživača krajnjeg korisnika na zlonamerni računar ili veb stranicu, korišćenjem alata za daljinski pristup i drugo.

3. Izvršenje neovlašćene transakcije. Ako prevarant poseduje kredencijale žrtve, on može obaviti transfer novca na bilo koji račun, a ako ih ne poseduje može primeniti automatizovani malver koji će i novac tokom transakcije između krajnjeg korisnika i finansijske institucije preusmeriti na drugu lokaciju. Jedan od postupaka poznat je kao *farming,* gde se legitimni veb sajtovi preusmeravaju na nove lokacije; ne koriste se prevare da korisnik sam oda vlastite podatke već zlonamerni kod koji se instalira na računar žrtve ili na server u računarskom sistemu. Instalirani kod preusmerava informacije koje se šalju preko mreže sa prave na lažnu adresu – sajt, bez pristanka i znanja korisnika. Na ovaj način nanosi se šteta žrtvi kod elektronskog bankarstva i plaćanja računa, pa se novac preusmerava na bankovne račune koji služe za krađu novca.

---

[12] „Sajber hronika", *Informacija*, 16.06.2016, http://www.informacija.rs/Sajber-hronika/Kralj-spama-koji-je-kompromitovao-pola-miliona-Facebook-naloga-osudjen-na-2-5-godine-zatvora.html:

„Kralj spama" je izvesni Senford Valas iz Las Vegasa, višestruko osuđivan zbog računarskih krađa i prevara, koji je, kao službenik firme Cyber Promotion, u jednom danu devedesetih godina prošlog veka poslao 30 miliona spam poruka.

[13] Viktor Kanižai, Zlonamerni softver dizajniran da omogući izvršavanje neovlašćenih transakcija, u *Zbornik radova ZITEH-16*, urednik Slobodan Petrović (Beograd: Udruženje sudskih veštaka za IT, 2016).http://www.itvestak.org.rs/wp-content/uploads /2015/11/Zbornik-radovaZITEH-16.pdf.

Poslednjih godina razvijeni su trojanci koji ne zahtevaju dodatni softver na računaru žrtve; oni funkcionišu nezavisno i za njihovo funkcionisanje je dovoljno da se zarazi računar ili telefon žrtve i da se ukrade novac.[14] Mogućnosti ovih trojanaca su i da kradu podatke sa kreditnih kartica ili da presreću komunikacije između klijenta i banke. Sa rastom funkcionalnosti mobilnih uređaja rastu i apetiti kriminalaca koji profitiraju korišćenjem mobilnog zlonamernog softvera, tako da se pretpostavlja da će se vremenom ovaj softver znatno usavršavati i da će trojanci još više napadati bankarske institucije.

Ransomver je vrsta malvera koji sprečava ili ograničava korisnicima da pristupe sistemu, zaključava ekran ili ne dozvoljava pristup pojedinim fajlovima računara. Smatra se da je to trenutno najopasnija vrsta malvera koja može da donese dosta koristi i novca kriminalcima. Većina softvera iz podgrupe ransomvera vrši šifrovanje datoteka određenog tipa na računaru žrtve, sa krajnjim ciljem traženja i dobijanja novca ili drugih usluga od žrtve u zamenu za ključ šifre. Novac koji se isplati nije garancija da je problem uspešno okončan i da će sistem nakon toga funkcionisati normalno ili da se napad neće ponoviti. Način instaliranja ransomvera je isti ili sličan kao kod drugih malvera, a mogu se instalirati na lične računare ili servere računarskih sistema. Većina ovog softvera je „useljena" u računare preko spam i-mejlova sa zlonamernim prilozima ili linkovima koji vode ka zaraženim veb stranicama. Samim postupkom instaliranja ransomvera preuzeti su i drugi podaci koji su bili dostupni na računaru, tako da se može očekivati i neki drugačiji napad.

Ova vrsta malvera je, po kvalitetu i broju modifikacija, u naglom usponu, tako da je broj ransomver napada u prvom kvartalu 2016. godine bio za oko 30% veći nego u poslednjem kvartalu 2015, ali je evidentirano i povećanje broja napada koji su usmereni prema IKT sistemima korporacija (17,2% od ukupnog broja napada).[15]

Jedan mehanizam krađe novca od banke[16]: Krađa novca od banke i njenih klijenata, korišćenjem ukradenog identiteta korisnika interneta ima sledeći scenario u pet koraka:

1. Pronalaženje većeg broja korisnika koji plaćaju račune preko interneta, za šta se koriste lako dostupne e-adrese i dobro osmišljene e-poruke čijim otvaranjem se instalira zlonamerni softver i osigurava pristup računaru žrtve (žrtava).

2. Kupovina specijalizovanog softvera (*exploit kits*) na crnom tržištu, potrebnog radi instaliranja specijalnih bankarskih trojanaca u računar žrtve. Ovakav softver se stalno razvija i usavršava i na crnom tržištu mu je cena od nekoliko stotina do preko hiljadu dolara.[17]

3. Instaliranje softvera sa bankarskim trojancima u računar žrtve posredstvom mreže i ranije instaliranog zlonamernog softvera.

4. Kada se računar žrtve, koji je pod kontrolom kriminalaca, koristi za elektronsko bankarstvo, a kriminalcima nisu poznati kredencijali žrtve, podaci koje šalje žrtva usmeravaju se na lažni server – tehnika napada sa računarom posrednikom ili metodom „čovek u sredini" (*man-in-the-middle – MITM*). Dok je korisnik uveren da je platio račun, novac je preusmeren i uknjižen na nekom računu koji je otvoren za krađu ili, što je češći

[14] Roman Unuchek i Victor Chebyshev. „Mobile malware evolution 2015", *Securelist*, 23.02.2016, https://securelist.com/analysis/kaspersky-security-bulletin/73839/ 2015.

[15] Isto.

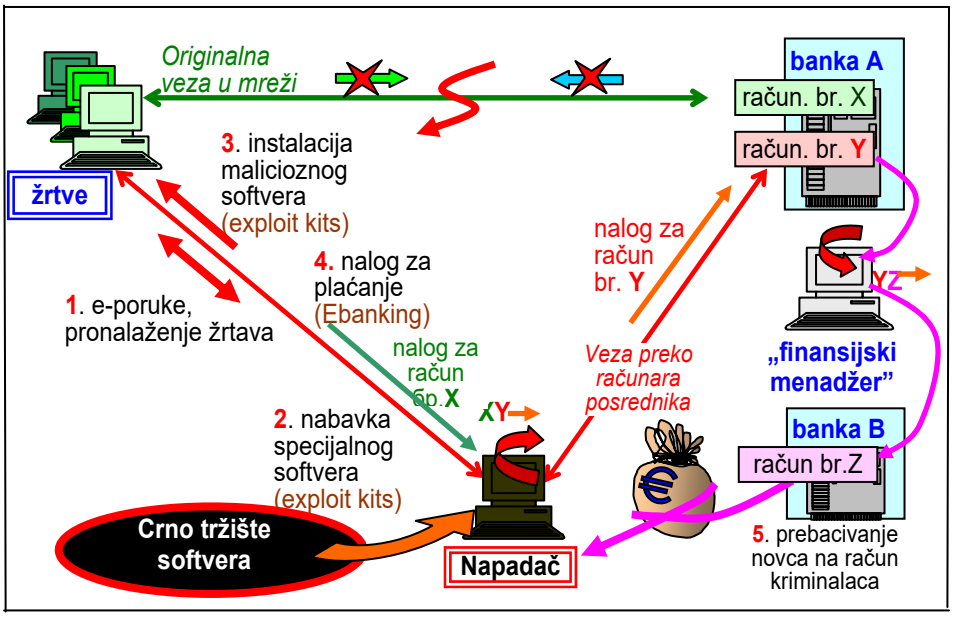
[16] Prema: „Kako opljačkati banku u 21.veku", *Informacija*, 07.12.2012, http://www.informacija.rs/ Clanci/ Kako-opljackati-banku-u-21-veku.html.

[17] „Moćni hakerski alati –exploit kits", I*nformacija*, 14.02.2011. http://www.informacija.rs/Virus/Mocni-hakerski-alati-exploit-kits.html.

slučaj, novac se uplaćuje na već postojeće legalne račune uz pristanak i za proviziju vlasnika računa *(money mules* – mule za prenos novca). Vlasnici računa za prenos novca regrutuju se posredstvom interneta radi obavljanja poslova sa primamljivim nazivima radnih mesta, kao što su „finansijski menadžer" ili „menadžera za prenos novca", a poslove obavljaju radeći kod kuće za ugovoreni honorar.[18] Ova lica obično ne znaju poreklo novca i uverena su da rade legalan posao i za legalnu firmu, a u stvari su saučesnici u izvršenju krivičnog dela.[19]

5. Sa svog legalnog računa i uz minimalnu nadoknadu „finansijski menadžer" brzo prebacuje novac na račune lopova, čime je delo i okončano.

Uprošćena šema izvršenja opisane krađe prikazana je na slici 2.



Slika 2 – *Šema krađe novca od banke (ili od klijenata banke) korišćenjem ukradenih identiteta, sa posrednim računarom (man-in-the-middle – MITM)*

[18] Europol, „Europe-wide action targets money mule schemes", Eurojust Web, 01.03.2016, http://www.eurojust.europa.eu/press/pressreleases/pages/2016/2016-03-01.aspx:
Prema objavi Europola od 01.03.2016, u vremenu od 22. do 26.02.2016. Europol, pravosudni i drugi organi više država EU, ali i nečlanica (Moldavija i druge) , udružilo je snage u akciji protiv „novčanih mula", a kao rezultat operacije bilo je identifiovanje skoro 700 lica za prenos novca, uhapšeno 81 lice, a otkriveni su i sprečeni značajni finansijski gubici i otkriveno preko 900 žrtava.nedozvoljenih transakcija.

[19] Cifas, „ 'Money Mules' more likely to be aged under 30", 08.12.2016. https://www.cifas.org.uk/ press_ centre/money_mules:
U prvih devet meseci 2016. u V.Britaniji je 73.503 individualnih bankovnih računa korišćeno za nelegalne transakcije novca, 39,4% imalaca legalnih računa su mlađi od 31 godine, dok su imaoci računa u dobi od 31 do 50 godina zastupljeni sa 38%.

Bez obzira na način na koji je neovlašćeno pristupljeno računaru krajnjeg korisnika, hakerisanje e-pošte smatra se za jedan od najefikasnijih prolaza u računarski prostor korisnika interneta i omogućava veoma razorne napade. Kada se zlonamerna poruka isporuči ranjivom računaru, tada je ispručen i zlonamerni kod, a on može da na računaru prikriveno instalira trojance (zlonamerni softver), da usadi crve (softver koji umnožava sam sebe, prenosi se kroz mrežu i preuzima kontrolu nad funkcijama računara), da zloupotrebi celokupan sistem ili da pokrene priloge e-pošte, što znači da može praktično sve.[20]

C) Krađa identiteta iz IKT sistema i mreža

Informaciono-komunikacioni sistem[21] je tehnološko-organizaciona celina koja obuhvata: elektronske komunikacione mreže; uređaje ili grupe međusobno povezanih uređaja gde se vrši automatska obrada podataka korišćenjem računarskog programa; podatke koji se pohranjuju, obrađuju, pretražuju ili prenose pomoću uređaja i mreža i organizacionu strukturu putem koje se upravlja IKT sistemom.

Neovlašćeno prikupljanje podataka iz velikih baza podataka (ili zbirki podataka) predstavlja nasilni upad u računarski sistem, Pri tome nisu ugroženi samo podaci o ličnosti, već i celokupno poslovanje korisnika računarskog sistema. U poređenju sa klasičnim kriminalom, ovaj postupak je istovetan nasilnom upadu u tuđe objekte, a poznat je pod pojmom hakerisanje ili haking (*hacking* – čovekov um protiv računara), iako sam pojam može označavati i pozitivne postupke kako bi se računar iskoristio na najbolji način. Ako se želi gruba podela načina krađe tuđih podataka iz IKT sistema, što haking kao metod i jeste, razlikuju se dva osnovna oblika realizacije ovog dela[22]:

1. Pribavljanje potrebnih informacija za upad u tuđi računarski sistem (sadržaji baza podataka, internet adrese, telefonski brojevi, parametri za indentifikaciju, lozinke i slično). Načini i metodi pribavljanja informacija su veoma različiti, a koriste se pretraživanje elektronske i druge pošte, novina i drugih publikacija, prisluškivanje, ispitivanje, metode socijalnog inženjeringa, podmićivanje, krađe i drugo. Za dobijanje potrebnih informacija neretko se koriste zaposleni u računarskim centrima koji, svojom nepažnjom, neznanjem ili sa namerom, doprinose lakšem upadu napadača u sistem. Na osnovu poznatih informacija upad u tuđi računarski sistem je znatno olakšan, a postupak je bezbedniji po napadača.

2. Teži način, ali nikako manje opasan i uspešan, zahteva veliko stručno znanje, strpljiv i dugotrajan rad napadača, kao i kvalitetniju opremu i softver. Metod se zasniva na postepenom pristupu sistemu preko softverskih barijera i drugih sistema zaštite po principu *„pokušaj, pogreši, nađi i otkloni grešku i ponovo pokušaj”*.

Kada se jednom „nađe” u sistemu, napadač može dodatno da koristi slabosti sistema i ostvari privilegovani pristup do svih potrebnih podataka i datoteka. Karakteristike hakinga su da je to dobro planiran, nedozvoljen i nasilan pristup, da je baziran na visokom profesionalnom znanju napadača i da je pri tome napadač, po pravilu, bezbedno udaljen od mesta upada u računarski sistem. Upad u sistem može se izvršiti i na samom serveru

[20] Stjuart Meklur (videti fusnotu 6), 558.

[21] NS RS. Zakon o informacionoj bezbednosti, *Sl. glasnik RS*, br.6/2016.

[22] Slobodan R. Petrović, (videti fusnotu 3), 196-197.

kada je hakeru potrebno da reši i problem prolaska kroz fizičke sisteme zaštite, gde su u prednosti zlonamerni pojedinci koji su zaposleni u ciljanoj firmi ili oni koji imaju pristup po drugom osnovu.

Krađa podataka o ličnosti na ovaj način ima za posledicu mnogo ukradenih podataka koji se mogu koristiti za razna krivična dela i naneti licima i firmama velike štete.[23] Velike krađe i-mejl adresa imaju za cilj stvaranje baze novih potencijalnih primalaca spam poruka i malvera radi dalje eksploatacije zaraženih računara.

Zbog navedenih mogućnosti i evidentnih pretnji, otkrivenih krađa identiteta i na osnovu njih realizovanih raznih prevara, prvenstveno bankarskih, dve trećine korisnika interneta u EU izražava zabrinutost za lične podatke koji se čuvaju kod državnih organa. Više od polovine građana EU zabrinuto je za svoje bankarske kartice i mogućnosti da budu žrtve drugih onlajn bankarskih prevara. To se potkrepljuje podatkom da je tokom 2014. godini u zemljama EU zabeležen nagli porast broja pokušaja instaliranja zlonamernog softvera ili pristupa računaru posredstvom e-pošte ili telefona i to na 47% aktivnih računara.[24]

Rasprostranjenost krađe identiteta

Krađa identiteta u svetu

Napadi na lične računare, gde su kao oblici najzastupljeniji malveri (trojanci, crvi), spam i fišing napadi, pokazuju tendenciju povećanja, kako po broju napada, tako i po narastanju broja različitih zlonamernih softvera koji se primenjuju. U toku 2015. godine prema izveštaju Laboratorije Kasperski[25], otkriveno je 2.961.727 štetnih instalacionih paketa malvera, 884.774 novih zlonamernih mobilnih programa (trostruko povećanje u odnosu na 2014) i 7.030 mobilnih bankarskih trojanaca. Broj novih malvera stalno raste, tako da je u periodu od 2003. do 2013. godine otkriveno oko 200 hiljada, 2014. godine oko 300 hiljada, a 2015. oko 900 hiljada novog malicioznog koda. Karakteristike novih malvera su takve da krajnji korisnik nije u stanju da ih eliminiše, kriminalci koriste razne metode za njihovo skrivanje, a u upotrebi su malveri koji kriminalcima daju potpunu kontrolu nad zaraženim računarom.

Tokom 2015. u svetu je registrovano oko 147 miliona fišing napada (napada na koje su se aktivirali antifišing sistemi, pa se može pretpostaviti da ih je bilo znatno više); od tog broja najviše napada je pretrpela Rusija (17,8%), dok su SAD bile najbolji „domaćin" napadačima i sa njene teritorije je izvršeno najviše napada (15,2%). Prema cilju, fišing napadi su najviše bili usmereni na onlajn finansijske institucije (banke, sistemi plaćanja i onlajn prodavnice).

---

[23] „Najveća krađa podataka u istoriji," *Telegraf*, 06.08.2014.http://www.telegraf.rs/hi-tech/internet/1181038-najveca-kradja-podataka:

Godine 2014. je objavljeno da je grupa ruskih hakera sa oko 420 hiljada sajtova svetskih kompanija ukrala podatke za oko 500 miliona i-mejl naloga. Obim krađe je otkriven nakon sedam meseci istraživanja firme *Hold Security*. Hakeri su prvenstveno napali baze podataka provajdera i-mejl usluga, društvene mreže i druge veb stranice kako bi došli do i-mejl adresa, a u drugoj fazi je sledilo slanje spam poruka i malicioznog softvera i krađa kompletnog identiteta, kako se pretpostavlja – za druge naručioce. Moguća šteta ove krađe do sada nije objavljena.

[24] European Commision (videti fusnotu 9).

[25] Anton Ivanov i dr. Overall statistics for 2015. u *Kaspersky Security Bulletin 2015 (Securelist* , 15.12.2015), https://securelist.com/files/2015/12/KSB_2015_Statistics_FINAL_EN.pdf,

Na povećani obim ugroženosti podataka o ličnosti ukazuju i sledeći podaci za 2015. godinu[26]:

– registrovano je 1.966.324 obaveštenja o pokušajima infekcija ličnih računara zlonamernim softverom radi krađe novca preko onlajn pristupa bankovnim računima;

– na 753.684 ličnih računara otkriven je ransomver, a 179.209 računara bilo je meta šifrovanja ovim softverom;

– 34,2% korisnika računara bilo je tokom godine izloženo najmanje jednom veb napadu;

– za napade je korišćeno 6.563.145 različitih računara.

Napadi na baze podataka. Na svetskom nivou tokom 2015. godine otkriveno je 1.505 upada u baze podataka[27], što je za oko 8% više nego prethodne 2014. godine. Napade su u velikom broju organizovali aktuelni ili bivši zaposleni u firmi (oko 65%svih napada).

Procena je da su tokom 2015. bili ugroženi podaci za oko milijardu ljudi[28], a samo u 21-nom napadu („mega napadi") bilo je ugroženo 814,5 miliona podataka o ličnosti, pored kojih se kao veoma uspešni napadi može svrstati i 55 napada koji su, svaki pojedinačno, ugrozili preko milion podataka o ličnosti. Kao posledica spoljnih hakerskih napada kompromitovano je oko dve trećine od ukupnog broja kompromitovanih podataka, ali je veliki broj podataka nekontrolisano „iscurio" zbog nemara ili namere zaposlenih.

Ako se razmatraju putevi kojima se neovlašćeno pristupa podacima o ličnostima ili drugim vrednim informacijama, najveći broj napada na baze podataka izveden je hakerskim napadima posredstvom interneta (46%), zatim preko krađe dokumenata (*paper documents*) (14%)[29], „gubitka" podataka zbog nemara ili namerno (8%), posredstvom e-poruka (7%) itd. Po oblastima rada najugroženije su kompanije koje se bave visokom tehnologijom (29%), obrazovne ustanove (20%), a zatim zdravstvo, bankarski sektor, saobraćaj i trgovina.

Spoljnim napadima najviše su ugrožene kompanije koje se bave visokom tehnologijom, trgovinom i saobraćajem, a unutrašnjim napadima najviše su ugroženi lični podaci u bankama, osiguranju i zdravstvu. Uopšteno, državne institucije su pretpele oko 17% od ukupno 1.505 napada, poslovne organizacije oko 73%, a ostale institucije i organizacije, uključujući i međunarodne organizacije – oko 10% napada. Karakteristika krađe podataka 2015. u svetu je da je najveći broj podataka otuđen u relativno malom broju napada (u 55 velikih i 21 mega napada), gde je kompromitovano blizu milijardu ličnih podataka. Najnoviji podaci pokazuju da se jednim hakerskim napadom mogu prisvojiti i podaci o znatno većem broju lica, pa čak i preko milijardu korisničkih naloga.[30]

---

[26] Isto.

[27] InfoWatch, „Global data leakage report 2015", 2016, http://infowatch.com/report2015.

InfoWatch je firma bliska firmi „Kaskerski Lab" sa sedištem u Rusiji i bavi se informacionombezbednošću i zaštitompreduzeća.

[28] Isto: Oko 191 milion podataka o biračima SAD dospelo je na internet zbog grešaka u bazi podataka.

[29] „Panamski papiri", *Blic*, 09.05.2016. http://www.blic.rs/vesti/svet/panamski-papiri-dokumenti-na-internetu-34-adrese-iz-srbije/ejht89e:

Najpoznatija provala u baze dokumenata u toku 2016. poznata je kao „Panamski papiri" i objavljena je preko nemačkog lista *Zidojče cajtung*. Obelodanjeno je oko 11,5 miliona dokumenata advokatske kancelarije „Mossack Fonseca" u kojima se nalaze podaci o poslovanju 214.000 ofšor firmi i njihova veza sa velikim brojem ljudi, značajnim u nacionalnim i/ili svetskim okvirima.

[30] „Najveći hakerski napad u istoriji", *Blic*, 15.12.2016, http://www.blic.rs/vesti/svet/najveci-hakerski-napad-u-istoriji-hakovani-podaci-vise-od-milijardu-korisnika-jahua/0hxjej7:

Kompanija Yahoo objavila je da je avgusta 2013. hakovano više od milijardu naloga korisnika te kompanije. Ukradeni su korisnički podaci koji sadrže imena, i-mejl adrese, brojeve telefona, datume rođenja, bezbednosna pitanja i odgovore koji se koriste za potvrdu indentiteta naloga. Ovo hakovanje otkriveno je posle 3,5 godina, a

Prema broju napada kojima su bile izložene baze podataka na teritorijama država prednjače SAD sa 859 napada, zatim Rusija (118), V. Britanija (112), Kanada (38), Nemačka (38), Australija (27), a slede ih Japan, Indija, J. Koreja i Austrija.[31]

Uprkos suprotstavljenim rezultatima analiza različitih organa koji se bave VT kriminalom i procenom izazvane štete usled upada organizovanih kriminalnih grupa u računarske sisteme i mreže, na osnovu podataka Centra za strateške i međunarodne studije (CSIS[32]) procenjuje se da je ta šteta na svetskom nivou u 2013. bila oko 445 milijardi dolara, odnosno između 375 i 575 milijardi dolara. Gubici koji se odnose na krađu intelektualne svojine iznose oko 160 milijardi dolara godišnje, a na krađu identiteta oko 150 milijardi dolara. U SAD oko 40 miliona ljudi je bar jednom u životu bilo žrtva krađe identiteta, dok je taj broj u Turskoj oko 54 miliona, u Nemačkoj oko 16 miliona, a u Kini više od 20 miliona ljudi.[33]

Krađa indentiteta u SAD

Na osnovu podataka o broju prekršaja i učinjenoj šteti od krađe podataka na teritoriji SAD u 2015. godini Federalna trgovinska komisija SAD (FTC)[34] izvela je globalni zaključak da krađa podataka o ličnosti u SAD, kao i svuda u svetu, doživljava ekspanziju. Ova komisija prati stanje u ovoj oblasti, pored ostalog, i prema broju centralizovano praćenih i analiziranih žalbi američkih građana.

U 2015. godini zabeležen je porast ukupnog broja žalbi građana SAD u odnosu na 2014. za oko 20%, tako da je ukupan broj žalbi bio oko 3 miliona ili oko 100 žalbi na 100 hiljada stanovnika. U ukupnom broju žalbi za 2015. najveću zastupljenost imaju žalbe za prevare koje su učinile kompanije prilikom naplata dugova potrošačima (29%), krađe identiteta (16%) i prevare koje su počinile varalice (11%).

Udeo žalbi zbog krađe identiteta u SAD, sa manjim oscilacijama, u stalnom je porastu, tako da je tokom 2015. zabeleženo 490.220 žalbi zbog krađe identiteta ili povećanje u odnosu na 2014. godinu od 47%. U strukturi krađe identiteta najviše prevara odnosi se na: prevare poreskih i drugih državnih organa (45%), prevare korišćenjem kreditnih kartica (16%) i prevare telefonskih i komunalnih kompanija (10%). Prevare banaka u ukupnom broju krađe identiteta zastupljene su sa 6%, kreditne prevare sa 4%, prevare radi zaposlenja sa 3%, a ostale vrste prevara ukupno su zastupljene sa oko 16%.[35]

---

po korišćenim metodima razlikuje se od napada iz 2014. kada je napadnuto 500 miliona naloga, kao i od napada u septembru 2016. godine.

[31] InfoWatch, „Global data leakage report 2015", 2016, http://infowatch.com/report2015

Podatak firme InfoWatch o broju napada u SAD (859 napada) razlikuje se od podatka koji je objavila Federalna trgovinska komisija SAD ((FTC) – 781 napad.

[32] CSIS – Center for Strategic and International Studies, http://csis.org/.

[33] Globana šteta od sajber kriminala iznosi 445 milijardi dolara, *B92*, 14.06.2014. http://www.b92.net/tehnopolis/internet.php?yyyy=2014&mm=06&nav_id=858832.

[34] FTC, „Annual Summary of Consumer Complaints",01.03.2016, https://www.ftc.gov/ news-events/press-releases/2016/03/ftc-releases-annual-summary-consumer-complaints.

FTC je dvopartijska federalna agencija koja se bavi zaštitom potrošača, podsticanjem investicija i konkurencije u SAD.

[35] Isto.

Pored navedenih podataka postoje procene da čak oko 15 miliona stanovnika SAD[36] ima probleme sa krađom identiteta u toku jedne godine, a ukupni gubici iznose više od 50 milijardi dolara, što znači da svaki ukradeni identitet povlači gubitak od oko 3.500 dolara.

Posebno su ugroženi podaci u bazama podataka državnih institucija i korporacija, a broj nedozvoljenih pristupa stalno raste, kao i materijalna šteta koju izazivaju krađe identiteta. Više od 100 miliona Amerikanaca svake godine je izloženo riziku zloupotrebe ličnih podataka koji se ukradu ili izgube iz državnih ili korporacijskih baza podataka. U 2015. godini prijavljen je 781 upad u baze podataka sa podacima za 169 miliona lica. Od toga je najviše upada bilo u računarske sisteme zdravstva (67%), vlade i vojske (20%).[37]

Prikazani podaci ne mogu u celini pokazati veličinu problema koji postoji sa VT kriminalom, jer ne uključuju mnoge institucije koje zbog konkurentnosti, očuvanja poverenja korisnika i sprečavanja sledećih upada (postaju prepoznatljiva meta) ne prijavljuju upade u svoje računarske sisteme i krađe identiteta. Mnoge upade administratori sistema i ne primete, tako da su procene da izneti brojčani podaci predstavljaju samo jednu trećinu stvarnog broja upada u računarske sisteme.

Krađa identiteta u Srbiji

Visokotehnološki kriminal je u stalnom porastu i u Srbiji, tako da je država bila prinuđena da zbog narastajućeg broja kriminalnih dela povezanih sa VT kriminalom, i u skladu sa potpisanom *Konvencijom o visokotehnološkom kriminalu,*[38] preduzme odgovarajuće mere radi poboljšavanja efekata borbe protiv ovog oblika kriminala.

Prema *Zakonu o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala*[39] iz 2005. godine, kojim se uređuje formiranje posebnih organizacijskih jedinica državnih organa radi otkrivanja, krivičnog gonjenja i suđenja za krivična dela VT kriminala, tokom 2006. formirana su posebna odeljenja za borbu protiv VT kriminala u okviru Republičkog javnog tužilaštva, MUP-a i Višeg suda u Beogradu.

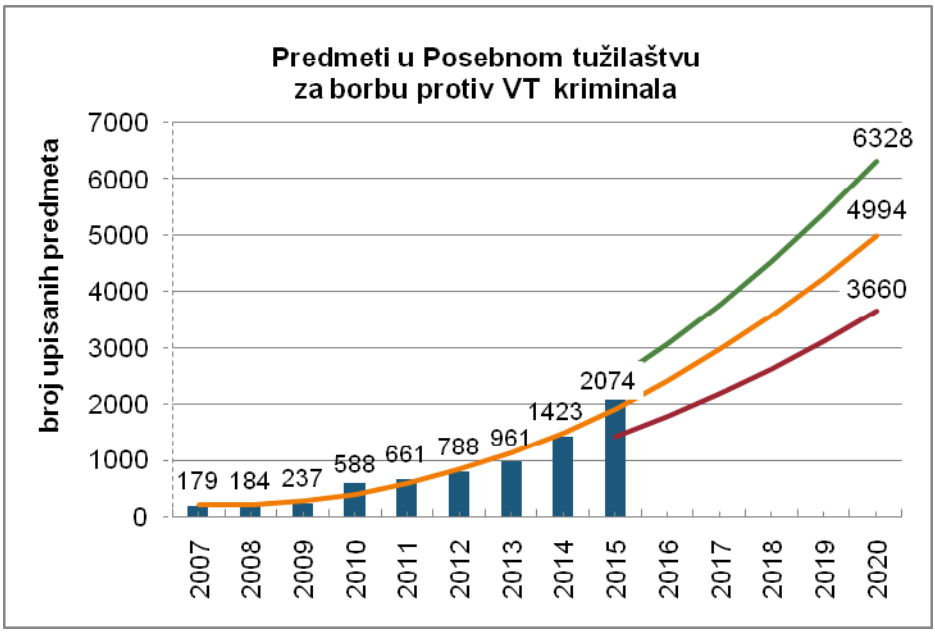
U posebnom odeljenju RJT – *Posebnom tužilaštvu za borbu protiv VT kriminala* od njenog osnivanja do 2015, broj upisanih predmeta u toku godine je u stalnom porastu, počevši od 179 predmeta u 2007. do 2074 predmeta u 2015. godini, prema grafikonu na slici 3.

[36] Rob Douglas, „Identity Theft Victim Statistics", *Identitytheft.info*, http://www.identitytheft.info/ victims.aspx.

[37] FTC (videti fusnotu 35).

[38] NS RS, „Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, *Sl.glasnik RS* – MU br. 19/2009. Konvencije je doneta u Savetu Evrope u Budimpešti 2001, od strane RS potpisana 2005. i ratifikovana 2009.

[39] NS RS, „Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala", *Sl.glasnik RS*, br. 6/2005 i 104/2009.



Slika 3 – *Pregled broja upisanih predmeta u Posebnom tužilaštvu za borbu protiv VT kriminala za period 2007–2015. godina sa trendom do 2020. godine*[40]

Na osnovu broja upisanih predmeta po godinama i uz pretpostavku da se ovakav trend nastavi, pokazalo se dobro slaganje empirijskih podataka sa pretpostavljenim paraboličnim trendom.[41] Sa verovatnoćom od 95% može se očekivati da u 2016. godini bude između 1.800 i 3.100, u 2017. između 2.200 i 3.800, a 2020. godini između 3.700 i 6.300 upisanih predmeta.[42]

[40] Podaci preuzeti iz: RJT, Rad javnih tužilaštava na suzbijanju kriminaliteta i zaštiti ustavnosti i zakonitosti u 2015. http://www.rjt.gov.rs/assets/Izvestaj za 2015.pdf.

[41] Svetozar Vukadinović, *Elementi teorije verovatnoće i matematičke statistike* (Beograd: Privredni pregled, 1981) , 415 – 444.

[42] Na osnovu poznatih podataka o broju upisanih predmeta po godinama za period 2007–2015, za $n=9$ godina sa ukupno $\sum_{i=1}^{i=9}\overline{BP_i}=7095$ upisanih predmeta, sledi da je aritmetička sredina $\overline{BP}=788$ predmeta godišnje, a na osnovu izvršenog proračuna trenda u odnosu na ishodišnu 2011. godinu $(g_{2011}=0)$ dobijena je jednačina paraboličnog trenda za broj predmeta $BP_i=585{,}3+215{,}8\,g_i+30{,}5\,g_i^2$, sa standardnom greškom $s=107$ predmeta, koeficijentom varijacije $V=0{,}139$ i koeficijentom regresije $r=0{,}98$ (odlično slaganje empirijskih i trend vrednosti). Trend vrednost za 2020. godinu $(g_{2020}=9)$ iznosi 4994 predmeta. ***Interval poverenja*** čine vrednosti između donje $D_i=BP_i(1-\alpha\cdot s/\overline{BP})$ i gornje $G_i=BP_i(1+\alpha\cdot s/\overline{BP})$ granice intervala poverenja,

Zbog narastanja broja kriminalnih dela u oblasti VT kriminala i nedovoljne sadašnje kadrovske popune Posebnog tužilaštva (tužilac, dva zamenika tužioca i tri pomoćnika tužioca), a radi jačanja kapaciteta organa nadležnih za borbu protiv VT kriminala, predviđeno je da se ovo odeljenje kadrovski ojača sa još dva zamenika tužioca i dva pomoćnika tužioca.[43]

Iz strukture krivičnih dela, prema podacima za četvorogodišnji period 2012–2015,[44] iz tabele 1 se vidi da je od ukupno 766 podnetih krivičnih prijava samo 125 prijava (16,3%) podneto za krivična dela iz Glave XXVII KZ[45] (krivična dela protiv bezbednosti računarskih podataka). Ostale prijave (83,7%) podnete su za krivična dela iz drugih područja KZ u kojima je korišćen računar ili računarska mreža, od čega je najviše dela povezano sa ugrožavanjem sigurnosti (čl. 138 KZ), prevara (čl. 208 KZ), pornografskim materijalom i iskorišćavanjem maloletnih lica (čl. 185 i 185b KZ) i autorskim pravima (čl. 199 KZ).

Tabela 1 – *Struktura krivičnih dela prema podnetim prijavama Posebnom tužilaštvu za borbu protiv VT kriminala za period 2012–2015. godina*

Struktura upisanih predmeta		Godina				∑	%
		2012.	2013.	2014.	2015.		
Poznati punoletni učinioci		114	160	294	198	766	14,6%
Nepoznati učinioci		65	243	770	570	1648	31,4%
Ostali predmeti		609	558	359	1306	2832	54,0%
Ukupno upisanih predmeta		788	961	1.423	2.074	***5.246***	100%
Struktura krivičnih dela (prijava) prema KZ za poznate punoletne počinioce		2012.	2013.	2014.	2015.	∑	%
Gl. XXVII Bezbednost računarskih podataka, KZ	Čl. 298: oštećenje pod. i progr.		2	2	1	5	16,3%
	Čl. 299: računarska sabotaža	2	2	3	4	11	
	Čl. 300: prav. i unošenje virusa	1		2	1	4	
	Čl. 301: računarska prevara	17	6	14	3	40	
	Čl. 302: nelegalan pristup mreži	8	5	34	17	64	
	Čl. 303. spreč. pristupa mreži			1		1	
Ukupno krivičnih dela za gl. XXVII KZ		28	15	56	26	125	
Ostala krivična dela prema KZ		86	145	238	172	641	83,7%
Svega krivičnih dela		114	160	294	198	766	100%
Broj počinilaca		144	185	332	226	887	
Broj počinilaca po krivičnom delu		1,26	1,16	1,13	1,14	1,16	

između kojih je smeštena tred-vrednost za tu godinu. Koeficijent α izražava stepen poverenja u granične vrednosti intervala i uz pretpostavku da se podaci rasipaju po normalnoj raspodeli za 95% poverenja (ili verovatnoće) pripadni koeficijent je: $\alpha = 1{,}96$. Sledi da su za 2020. granice poverenja $D_{2020} = 3660$ i $G_{2020} = 6328$, što znači da će broj upisanih predmeta, uz ostale nepromenjene uslove, biti između 3.700 i 6.300 sa verovatnoćom od oko 95%, kao što pokazuje i grafikon na slici 3.

[43] RJT (videti fusnotu 41).

[44] RJT, Rad javnih tužilaštava na suzbijanju kriminaliteta i zaštiti ustavnosti i zakonitosti u 2012. (isto za 2013, 2014. i 2015). http://www.rjt.gov.rs/assets/Izvestaj za 2012.pdf(isto za 2013, 2014. i 2015).

[45] NS RS – Narodna skupština Republike Srbije. „Krivični zakonik”, *Sl.glasnik RS*, br. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012,104/2013 i 108/2014.

Za krivična dela direktno povezana sa bezbednošću računarskih podataka (glava XXVII KZ) najveći broj prijava podnet je za neovlašćen pristup računarskim mrežama (čl. 302 KZ) i za prevare (čl. 301 KZ) – oko 83,2%, što navodi na zaključak da su pod ova krivična dela podvedena i dela krađe identiteta, jer naš KZ ne poznaje ovu vrstu krivičnog dela. Ako se uporedi broj izvršilaca krivičnih dela sa brojem krivičnih dela (887/766=1,16) može se izvesti zaključak da su dela koja su procesuirana zbog korišćenja računarske tehnike, uglavnom, izvršavali pojedinci.

Zaključak

Sigurno je da će IKT u budućnosti uticati na svaki deo našeg života, što će doprineti i razvoju nauke i boljem životu, ali uporedo s tim, zbog brzog razvoja i usavršavanja metoda i tehnika izvršenja krivičnih dela, koja u osnovi imaju upotrebu računara i računarskih mreža, prvenstveno globalne računarske mreže – interneta, povećavaju se pretnje i opasnosti od raznih vrsta zloupotreba.

U radu je obrađena krađa identiteta, kao pojavni oblik VT kriminala, sa pokušajem da se prezentuje njihovo osnovno razvrstavanje prema karakterističnim pokazateljima o načinima i tehnikama izvršenja dela, formama korišćena otuđenih podataka i rasprostranjenosti. Krađa identiteta, koja se zasniva na zloupotrebi podataka pojedinaca, može da nanese veliku materijalnu i/ili nematerijalnu štetu žrtvama, tako da se zaštiti podataka mora pokloniti dužna pažnja. Korišćenje interneta pogoduje razvoju krađe identiteta sa ličnih računara i iz IKT sistema i mreža, čemu često doprinosi i nemaran odnos operatera koji rukuju bazama podataka o ličnosti.

U naglom porastu je broj i kvalitet malvera, tako da je tokom 2015. otkriveno oko 900 hiljada novih malicioznih kodova. Posebno je u razvoju malvera postignut napredak u modifikacijama ransomvera kojima se vrši sprečavanje ili ograničavanja upotrebe računara ili IKT sistema, a osnovni cilj je da se uceni korisnik (potraživanje novca ili drugih vrednosti), kao protivusluga za dobijanje šifre ili ključa za skidanje ograničenja na računaru ili IKT sistemu.

Iz velikih baza podataka, pored ranije primenjivanih metoda da se prvo prikupe željene informacije za napad na IKT sistem, sve je prisutnija povećana agresivnost hakera koji se udružuju i kradu podatke iz baza sa milionskim zapisima, a radi njihove dalje kriminalne eksploatacije. U svetu su prošle godine bili ugroženi podaci od skoro milijardu osoba, evidentirano je oko hiljadu i po upada u baze podataka velikih organizacija i korporacija, a šteta se procenjuje na iznos između 375 i 575 milijardi dolara, od čega je oko 150 milijardi dolara nastale štete kao posledica krađe identiteta. Najnoviji podaci pokazuju da se samo jednim hakerskim napadom na velike kompanije (Yahoo, 2013) koje čuvaju podatke o ličnostima može kompromitovati i preko milijardu korisničkih naloga sa ličnim podacima. Zbog narastanja mogućnosti i širenja kriminala zasnovanog na krađi identiteta, raste i zabrinutost korisnika interneta za vlastite podatke i njihovu zloupotrebu. Tako je u zemljama EU u 2015. dve trećine korisnika iskazalo zabrinutost za sigurnost svojih podataka i moguću krađu, a skoro polovina svih ličnih računara bilo je izloženo napadima i pokušaju instaliranja zlonamernog softvera radi zloupotrebe podataka korisnika računara.

Izneti podaci o porastu broja kriminalnih dela u oblasti VT kriminala zahtevaju promenu svesti o njegovoj opasnosti i preduzimanje potrebnih mera za povećanje bezbednosti ličnih računara i mobilnih uređaja kod pojedinaca i IKT sistema i mreža kod institucija.

U Srbiji je, kao i u većini zemalja u svetu, u povećanju broj otkrivenih i procesuiranih krivičnih dela povezanih sa upotrebom informaciono-komunikacione tehnologije, što dodatno obavezuje i državne organe za sistemsko rešavanje problema zaštite IKT sistema i mreža na svom sajber prostoru. To je posebno važno, uz saznanje da je VT kriminal nezavisan od geografskih i administrativnih ograničenja, te da je od njega neophodna zaštita i suprotstavljanje i na prostoru izvan državne teritorije, što podrazumeva aktivnu saradnju organizacija za borbu protiv VT kriminala na globalnom nivou. Poseban segment zaštite čini preventivno delovanje državnih i drugih institucija kako bi se zaštitili IKT sistemi od posebnog značaja za državu, a u slučaju napada izvršilo smanjenje štete i sanacija posledica.

Literatura

[1] Vukadinović, Svetozar. *Elementi teorije verovatnoće i matematičke statistike*. Beograd: Privredni pregled, 1981.

[2] „Globana šteta od sajber kriminala iznosi 445 milijardi dolara", *B92*, 14.06.2014, http://www.b92.net/tehnopolis/internet.php?yyyy=2014&mm=06&nav _id=858832. (pristupljeno: 10.10.2016).

[3] Douglas, Rob. „Identity Theft Victim Statistics", *Identitytheft.info*, http://www.identitytheft.info/victims.aspx. (pristupljeno 23.11.2016).

[4] European Commision. „Ciber security report 2014", *Special Eurobarometer 423*, februar 2015. http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf.

(pristupljeno: 01.12.2016).

[5] Europol. „Europe-wide action targets money mule schemes". Eurojust Web, 01.03.2016, http://www.eurojust.europa.eu/press/pressreleases/pages/2016/2016-03-01.aspx (pristupljeno: 10.12.2012).

[6] InfoWatch. „Glogal data leakage report 2015", 2016, http://infowatch.com/report2015. (pristupljeno: 12.12.2016).

[7] Ivanov, Anton,Denis Makrushin, Jornt van der Wiel, Maria Garnaeva i Yury Namestnikov. „Overall statistics for 2015" u*Kaspersky Security Bulletin 2015*, *Securelist*, 15.12.2015, https://securelist.com/files/2015/12/ KSB_2015_ Statistics_

[8] FINAL_EN.pdf, (pristupljeno: 12.11.2016).

[9] „Kako opljačkati banku u 21.veku", *Informacija*, 07.12.2012, http://www.informacija.rs/Clanci/Kako-opljackati-banku-u-21-veku.html(pristupljeno: 01.12.2016).

[10] Kanižai, Viktor. Zlonamerni softver dizajniran da omogući izvršavanje neovlašćenih transakcija, u *Zbornik radova ZITEH-16*, urednik Slobodan Petrović, Beograd: Udruženje sudskih veštaka za IT, 2016. http://www.itvestak.org.rs/wp-content/uploads /2015/11/Zbornik-radovaZITEH-16.pdf, (pristupljeno: 10.12.2016).

[11] Meklur, Stjuart, Džoel Šambri i Džordž Kurtc. Hakerske *tajne: zaštita mrežnih sistema*, prevod Dejan Smiljanić i Milenko Šućur, Beograd: Mikro knjiga, 2006.

[12] „Moćni hakerski alati –exploit kits*", Informacija*, 14.02.2011, http://www.informacija.rs/Virus/Mocni-hakerski-alati-exploit-kits.html (pristupljeno: 16.11.2016).

[13] „Najveća krađa podataka u istoriji," *Telegraf*, 06.08.2014. http://www.telegraf.rs/hi-tech/internet/1181038-najveca-kradja-podataka. (pristupljeno: 10.11.2016).

[14] „Najveći hakerski napad u istoriji", *Blic*, 15.12.2016, http://www.blic.rs/vesti/svet/najveci-hakerski-napad-u-istoriji-hakovani-podaci-vise-od-milijardu-korisnika-jahua/0hxjej7. (pristupljeno: 15.12.2016).

[15] NS RS – Narodna skupština Republike Srbije. „Krivični zakonik*", Sl. glasnik RS*, br. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012,104/2013 i 108/2014.

[16] NS RS – Narodna skupština Republike Srbije. „Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala", *Sl. glasnik RS*, br. 6/2005 i 104/2009.

[17] NS RS – Narodna skupština Republike Srbije. „Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu*, Sl. glasnik RS* – MU br. 19/2009.

[18] NS RS – Narodna skupština Republike Srbije. „Zakon o zaštiti podataka o ličnosti", *Sl. glasnik RS*, br. 97/2008,104/2009, 68/2012 i 107/2012.

[19] NS RS – Narodna skupština Republike Srbije: „Zakon o informacionoj bezbednosti", *Sl. glasnik RS*, br. 6/2016.

[20] „Panamski papiri", *Blic.* 09.05.2016. http://www.blic.rs/vesti/svet/panamski-papiri-dokumenti-na-internetu-34-adrese-iz-srbije/ejht89e. (pristupljeno: 01.11.2016).

[21] Petrović, Slobodan R. *Kompjuterski kriminal*. Beograd: Vojnoizdavački zavod, 2004.

[22] RJT – Republičko javno tužilaštvo. Rad javnih tužilaštava na suzbijanju kriminaliteta i zaštiti ustavnosti i zakonitosti u 2012, 2013, 2014, 2015, http://www.rjt.gov.rs/assets/Izvestaj za 2012.pdf (isto za 2013, 2014, 2015). (pristupljeno: 10.12.2016).

[23] RZS – Republički zavod za statistiku. „Upotreba informaciono- komunikacionih tehnologija u Republici Srbiji u 2016. godini", 2016. http://webrzs.stat.gov.rs/ WebSite/repository/documents/00/01/50/47/ICT2014s.pdf. (pristupljeno: 10.12.2016).

[24] RZS – Republički zavod za statistiku. „Upotreba informaciono- komunikacionih tehnologija u Republici Srbiji u 2014. godini", 2014. http://webrzs.stat.gov.rs/ WebSite/repository/documents/00/01/85/78/ICT2014s.pdf. (pristupljeno: 10.12.2016).

[25] „Sajber hronika". *Informacija*, 16.06.2016, http://www.informacija.rs/Sajber-hronika/Kralj-spama-koji-je-kompromitovao-pola-miliona-Facebook-naloga-osudjen-na-2-5-godine-zatvora.html. (pristupljeno: 16.11.2016).

[26] „Ukrali 130 miliona kreditnih kartica*". Politika*, 18.08.2009. http://www.politika.rs/sr/clanak/100340/Ukrali-130-miliona-kreditnih-kartica. (pristupljeno: 11.11.2016).

[27] Unuchek, Roman, i Victor Chebyshev. „Mobile malware evolution 2015", *Securelist*, 23.02.2016, https://securelist.com/analysis/kaspersky-security-bulletin/73839/ 2015, (pristupljeno: 12.12.2016).

[28] FTC – The Federal Trade Commission. „Annual Summary of Consumer Complaints",01.03.2016, https://www.ftc.gov/news-events/press-releases/2016/03/ftc-releases-annual-summary-consumer-complaints. (pristupljeno 20.11.2016).

[29] Cifas. „Identity Fraud", https://www.cifas.org.uk/identity_fraud. (pristupljeno: 20.12.2016).

[30] Cifas. „'Money Mules' more likely to be aged under 30", 08.12.2016. https://www.cifas.org.uk/press_centre/money_mules (pristupljeno: 20.12.2016).