Skimming naprave v sloveniji

David Gracer, študent, Fakulteta za varnostne vede, Univerza v Mariboru

Namen prispevka
S prispevkom bom poskušal prikazati, kako deluje naprava za presnemavanje magnetnega zapisa bančnih, kreditnih in drugih kartic, oziroma v nadaljevanju tako imenovana "skimming" naprava. Opisal bom njene dele in delovanje le teh, kako delujejo storilci in na kak način izvedejo tovrstna kazniva dejanja, varnostne ukrepe pri uporabi bankomatov in ukrepe po ugotovitvi zlorabe vaše bančne kartice.

Metode
Prispevek temelji na avtorjevem poznavanju tovrstne kriminalitete in delovanja samega sistema. Prav tako je bila za preveritev trenutnega stanja poznavanja in seznanjenosti ljudi s tovrstnim pojavom izvedena anketa.

Ugotovitve
Ljudje skimming naprave na bankomatih v veliki večini ne bi prepoznali, klub temu, da bankomate uporabljajo skorajda vsakodnevno. Ne vedo, ali je uporaba bankomata varna ali ne, menijo pa, da se s pomočjo skimminga zgodi veliko kriminala. Varnost bankomatov v Sloveniji in Evropi je slaba, antiskimming naprave ne delujejo kot je potrebno, video nadzor ne pokriva vseh bankomatov, naprave, katere uporabljajo storilci pa so vedno boljše.

Praktična uporabnost
Prispevek daje ogromno splošnih informacij, ki bi zanimale uporabnike bankomatov in informacij glede uporabe bankomata, varnostnih ukrepov za varno uporabo bankomatov, oziroma prepoznave skimming naprave in s tem zmanšanje števila kaznivih dejanj s tega področja.

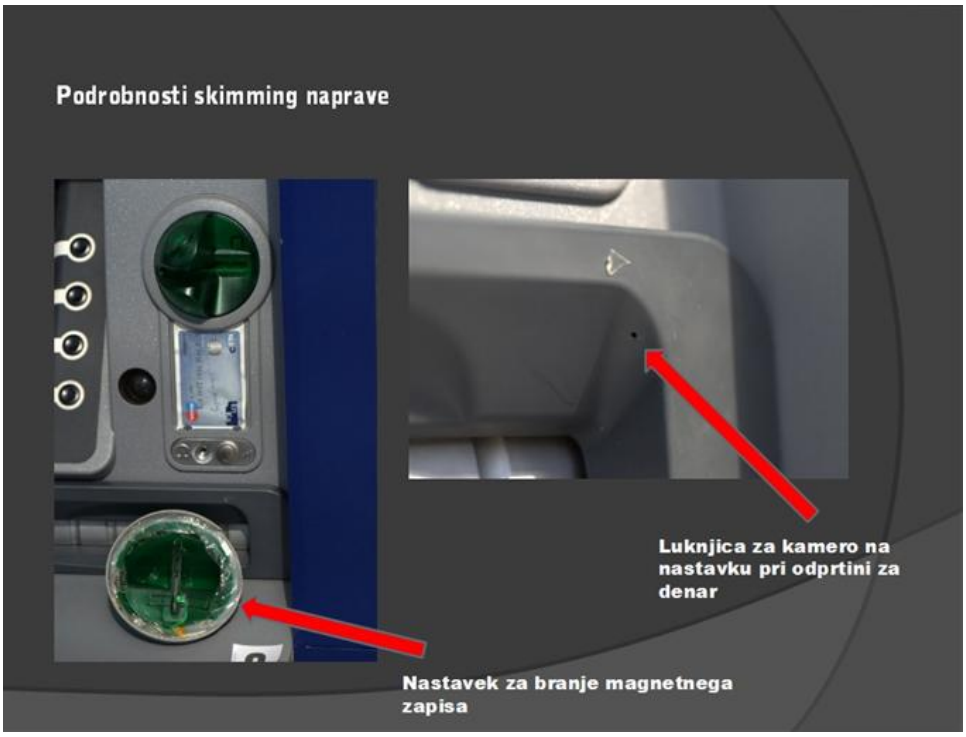
Izvirnost/pomembnost prispevka
Prispevek je namenjen vsem, ki uporabljajo bančne avtomate in do sedaj niso bili dobro obveščeni kako skimming deluje in zgleda. Predvsem pa tistim, ki bi s tem znanjem in uporabo bančnih avtomatov želeli prispevati k varnosti in preprečevanju zlorab bančnih kartic.

Ključne besede: magnetni zapis, PIN številka, bančni avtomat, skimming naprava, varnostni ukrepi.

1 UVOD

Sistem naprave je ponavadi zgrajen iz dveh delov. Prvega sestavlja del, ki zajem podatke o magnetnem zapisu bančnih kartic. Zajem magnetnega zapisa kartic je izveden s preureditvijo komercialnih prenosnih čitalcev magnetnih kartic z vgrajenim pomnilnikom, ki glede na velikost številk, katere zajema sam magnetni zapis lahko shrani več tisoč magnetnih zapisov, ne da bi ga bilo potrebno zamenjati. Ker odčitava magnetni zapis mora biti nekje v bližini reže za vstavljanje kartic. Magnetni senzor se ponavadi nahaja tik nad odprtino, kamor kartico vstavimo. Vgrajen je na notranji strani plastike, ki je izdelana tako, da se prilega originalni reži za vstavljanje bančnih kartic in jo je izredno težko opaziti, saj je popolnoma enake barve in od originalne reže odstopa približno dva do tri milimetre (Walters, 2009).
Drugi del naprave sestavlja del za vizualni zajem PIN številk bančnih kartic. Video zajem številke PIN je izveden s preureditvijo komercialnih miniaturnih kamer, kjer so ohranjeni vsi moduli za zajem in lokalno upravljanje (kamera, mikrofon, tipke). Najpogosteje je del, ki vsebuje sistem za zajem PIN številk vgrajen nekje v bližini tipkovnice, na katero je kamera tudi usmerjena. Lahko je skrita za plastiko, ki je izdelana tako, da se prilega odprtini za denar, na njej pa je izvrtana luknjica za mikro kamero, ki snema pritisnjene tipke ob vnosu številke PIN. V času, ko storilci tovrstnih kaznivih dejanj še niso bili tako izkušeni in niso imeli tako dobre opreme, so za snemanje PIN številke uporabnikov

bankomatov uporabili mobilni aparat, katerega so enostavno zalepili za rob na vrhu bankomata, tako da le-ta ni bil viden, ter vklopili snemanje (Walters, 2009).



Slika 1: Skimming naprava najdena na bankomatu v Sloveniji (Vir: Skimming, 2011)

Oba sistema delujeta avtonomno s pomočjo vgrajene Li-Ion polnilne baterije in podatke shranjuje lokalno v t.i. "flash" spomin. Ker se na bankomatu pojavi v kratkem obdobju sorazmerno veliko kartic, je na obeh delih sistema vgrajen časovnik, s pomočjo katerega je mogoče kasneje časovno uskladiti magnetni zapis z vneseno PIN številko.
Obstaja možnost, da ima oprema možnosti za brezžični prenos zbranih podatkov, kar pomeni, da lahko podatke iz samega bankomata storilci tovrstnih kaznivih dejanj zajemajo brezžično, torej s pomočjo prenosnega računalnika ali mobilnega telefona. Za branje podatkov večine naprav pa je potrebna odstranitev opreme z bančnega avtomata in priključitev na računalnik.

2 SISTEM DELOVANJA STORILCEV

Bančne kartice so vedno zlorabljene v tujini, kar kaže na to, da se s tovrstnimi dejanji ukvarjajo dobro organizirane in dobro medsebojno povezane skupine posameznikov in s prav tako dobro opremo, predvsem elektronsko za prenos in izdelavo samih ponarejenih kartic. Tako storilec na območju Slovenije po odstranitvi naprave, z le-te presname podatke o magnetnih zapisih kartic, katerim priloži posnetke oziroma PIN številke. V tujini se izdelajo bančne kartice z identičnim magnetnim zapisom, ki pa kot rečeno služijo za dvige na bančnih avtomatih ali za zlorabo na prodajnih mestih (POS terminali). Pri tem pa nastajajo visoke materialne škode, katere doletijo slovenske banke. Dejstvo je tudi, da mora skupina delovati hitro, predvsem od trenutka prve zlorabe naprej, saj slovenska družba Bankart d.d. pri spremljanju transakcij ugotovi, da je bilo v tujini na določenem bankomatu ali POS terminalu v kratkem času uporabljeno večje število bančnih kartic slovenskih imetnikov. Po ugotovitvi sumljivih transakcij v tujini nemudoma preveri, na katerem bankomatu v Sloveniji so bile bančne kartice uporabljene, ter obvešča banko izdajateljico kartic, katera takoj za tem prekliče vse bančne kartice, ki so bile v določenem času uporabljene na bankomatu, za katerega se sumi, da je bila na njem nameščena skimming naprava.

3 VARNOSTNI UKREPI PRI UPORABI BANKOMATA

Naprava za presnemavanje magnetnega zapisa bančnih, kreditnih in drugih kartic oz. tako imenovana skimming naprava, je na bankomat nameščena na način, da je za uporabnike bankomata praktično neopazna. Obstaja možnost, da uporabnik prepozna napravo, kadar odtenek barve naprave ni identičen barvi bankomata. Torej v primeru, da uporabnik opazi, da se ne ujemata barva bankomata z barvo dela plastike, kjer je reža za bančno kartico, ali reže za izdajo bankovcev in ob dotiku omenjenih delov začuti, da niso trdno pritrjeni na bankomat nemudoma pokliče policijo, naprave pa se čim manj dotika. Namreč deli naprav na bankomat niso pritrjeni zelo trdno in lahko uporabniku ostanejo v rokah že ob malo močnejšem prijemu. Zato je priporočljivo, da si človek pred uporabo bankomata vzame sekundo časa in malo močneje prime za del na katerem je reža za vstavitev bančne kartice ali reža za izdajo bankovcev. Bankomati so narejeni tako, da se pri tem nebi smelo nič premakniti, v primeru da je nanj nameščena skimming naprava pa bo ob močnejšem prijemu uporabniku skoraj zagotovo ostala v rokah.
Najbolj je potrebno biti pozoren ob vnosu PIN številke, katera je potrebna za nadaljno zlorabo bančne kartice. Bistvo naprave je torej, da jo storilec namesti na mesto od koder bo imela kamera jasen oziroma čist pogled na številčnico bančnega avtomata. Naprava je nastavljena tako, da posname vnos PIN številke tudi v primeru, ko uporabnik z rokama pokriva številčnico. Zato je v večini primerov naprava namešča diagonalno, pod ostrim kotom, tako da je kljub pokritju številčnice še vedno možen pogled na njo. Iz tega sledi, da je kamera največkrat nameščena kar na dodatnem okvirju, ki se ga pritrdi na režo za izdajanje bankovcev. Pri natančnem pregledu bankomata, pa je možno opaziti, da je nekje na delu reže za izdajo bankovcev zvrtana luknjica za mikro kamero, katera je lahko premera samo milimeter. Za shranjevanje podatkov o PIN številkah je prav tako možna prirejena tipkovnica, ki zgleda kot prava in je nalepljena čez originalno tipkovnico bankomata. Ob močnejšem prijemu od strani, se bi naprava morala odlepiti. V primeru, da uporabnik bankomata opazi, da je na katerem koli delu bankomata izvrtana luknjica ali je čez opazil dodatno tipkovnico, o tem takoj obvesti policijo. (Schultz, 2010).
Da bi bila skimming naprava na bankomatu čim manj vidna s strani uporabnikov, nanjo, oziroma na njene dele storilci na primer namestijo nalepke, različnih varnostnih služb, bank in podobno. Precej očitno je, da je na slovenskem bankomatu nalepka kakega tujega varnostnega podjetja ali banke, kar pa ponavadi uporabnik spregleda, saj na to ni pozoren.

4 UKREPI PRI UGOTOVITVI ZLORABE

Skimming naprave storilci nameščajo na bankomate, na katerih je velika frekvenca uporabe (center večjih mest, nakupovalna središča, itd..), zato so skrbi, da bo naprava v vašem kraju kjer živite ni potrebno bati, pazljivost pa kljub temu ni odveč. V primeru, ko opazite, da na vašem bančnem računu neupravičeno manjka denar, o tem obvestite svojo banko. Ko je nesporno ugotovljeno, da je do zlorabe bančne kartice prišlo, banka svojemu komitentu denar povrne, o tem pa obvesti policijo. Zato banke podajo kazensko ovadbo za vse, ki so bili "žrtve" skimminga in uporabnikom zlorabe ni potrebno posebej prijavljati na policiji (Predanič 2011).

5 ZAKLJUČEK

Seveda obstaja več vrst pridobitev magnetnega zapisa in varnostne PIN številke bančnih kartic. Tako poznamo skimming na bančnih avtomatih, POS terminalih, tatvine podatkov o karticah preko spleta. V zadnjem času so nepridipravi odkrili nov način pridobivanja podatkov iz bančnih kartic in sicer z uporabo naprave, ki iz banče kartice odčita čip. Uporaba tovrstne naprave je najbolj nevarna od vseh ostalih, saj se v čipu skrivajo podatki tako o magnetnem zapisu, kot o varnostni PIN številki bančne kartice. S tem storilcem kaznivih dejanj povezanih s skimmingom ni več potrebno predelovati ogmorne mase podatkov in usklajevati magnenih zapisov in PIN številk bančnih kartic, saj si pridobijo vse potrebne podatke sočasno. Zaenkrat se taka naprava v Sloveniji ni pojavila, v prihodnosti pa jo lahko pričakujemo in s tem še večje število zlorabljenih bančnih kartic.

Težave s skimmingom se zadnjih nekaj let pojavljajo po vsem svetu. V letu 2011 je ta pojav povečano dosegel tudi Slovenijo. Zaradi slabe varnosti bankomatov, slabih antiskimming naprav in video nadzora tovrstnim kaznivim dejanjem ni videti konca. Tovrstna kazniva dejanja je mogoče raziskovati izključno po storitvi, saj se ugotovijo, takrat ko je že prišlo do zlorabe bančnih kartic v tujini, zato je storilce toliko težje prijeti. V ta namen je bila v Sloveniji ustanovljena posebna skupina kriminalistov, ki se ukvarja s to problematiko (A.L., 2011).

Banke si prizadevajo izboljšati varnost bankomatov, vendar zaenkrat ni videti prave rešitve zoper boja proti skimmingu. Izboljšanje video nadzornega sistema organom pregona poveča možnost izsleditve storilcev, ne preprečuje pa kaznivih dejanj. Antiskimming naprave ne delujejo kot bi bilo pričakovati, oziroma je za skimming naprave uporabljena vedno boljša tehnologija. Trenutno najboljša rešitev je ozaveščenost uporabnikov, hitro ukrepanje družbe Bankart in učinkovito delo organov pregona.

Viri

Chris Walters, 19.4.2009, How ATM card skimming works, pridobljeno 21.12.2011, na http://www.crikey.com.au/2009/03/30/how-atm-card-skimming-works/

Jennifer Saranow Schultz, 12.8.2010, How to spot an A.T.M. skimmer, pridobljeno 23.12.2011, na http://bucks.blogs.nytimes.com/2010/08/12/how-to-spot-an-a-t-m-skimmer/

A.L., 7.12.2011, Slovencem s kartic pokradli pol milijona evrov, pridobljeno 25.12.2011, na http://www.slovenskenovice.si/crni-scenarij/doma/slovencem-s-kartic-pokradli-pol-milijona-evrov

Jure Predanič, 04.12.2011 kronika, Banka žrtvam povrne denar, pridobljeno 25.12.2011 http://www.delo.si/gospodarstvo/makromonitor/banka-zrtvam-povrne-denar.html

Skimming naprava najdena na bankomatu v Sloveniji, pridobljeno 25.12.2011, na http://www.genspot.com/PhotoGallery/Album.aspx?album_id=17216