CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Partnerka - kriminalna Internet organizacija

NCERT-PUBDOC-2011-09-331

Nacionalni CERT

Sadržaj

1 Uvod

Zasigurno ste već mnogo puta bili suočeni s primanjem neželjene elektroničke pošte, čitanjem komentara na web stranicama, forumima i društvenim mrežama koji reklamiraju farmaceutske proizvode, pornografske stranice, replike skupocjenih satova ili pak sadrže poveznice koje vode na malver. Iako je razvijena cijela anti-spam industrija, spam i dalje postoji i to ne samo u obliku elektroničke pošte.

Međutim, malo kome je poznata organizacija koja stoji iza tog milijunskog biznisa. Iza cijelog tog kriminalnog posla stoje stotine dobro organiziranih mreža koje su poznate pod ruskim imenom „partnerka“, s obzirom da najveći broj takvih organizacija dolazi iz Rusije. Mreže su ustrojene hijerarhijski, a na najnižoj razini nalaze se pojedinci zaduženi za web marketing. Takvi pojedinci su privučeni dobrom zaradom koju mogu ostvariti radom od kuće, a loša globalna ekonomska situacija ih privlači sve više i više. Cijeli kriminalni posao tog tipa ostvaruje milijunske profite, a podržan je od strane web hosting, ISP tvrtki i banki koje toleriraju takav oblik posla. Upravo iz tog razloga, posljednje dvije godine su sigurnosni stručnjaci i njihove organizacije koncentrirane na zatvaranje takvih tvrtki.

Ovaj dokument daje uvid u organizaciju takvih kriminalnih skupina i načine kojima dolaze do milijunskih zarada.

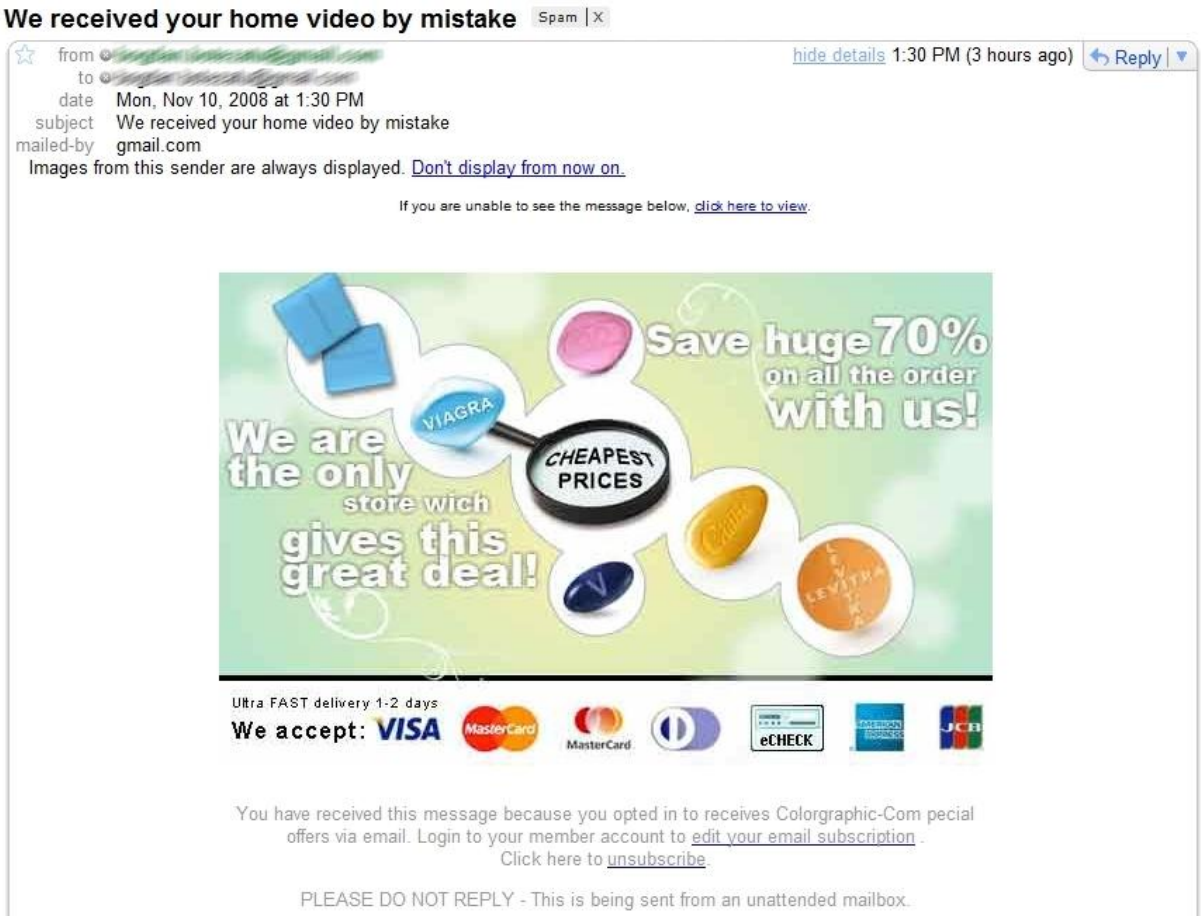
2 Tehnike generiranja web prometa

Kako bi došli do financijske koristi, kriminalci moraju reklamirati svoje „proizvode“, a to čine putem tzv. „crnog“ marketinga. Cilj im je imati što veći promet na svojim web sjedištima jer to obično znači i imati veći broj posjetitelja, odnosno kupaca. U svrhu generiranja prometa na svojim ilegalnim web sjedištima, kriminalci koriste različite tehnike. Osim širenja ogromne količine spama, one uključuju i tzv. „black-hat“ SEO (Search Engine Optimization), korištenje malvera te različite kombinacije navedenih tehnika.

2.1 Spam

Slanje spam poruka, najviše putem elektroničke pošte, ali i elektroničkih foruma, blogova, socijalnih mreža, servisa za izravnu komunikaciju itd. glavni je način reklamiranja proizvoda partnerki. Da bi spameri mogli slati neželjene poruke, potrebno im je pribaviti e-mail adrese potencijalnih primatelja. Najčešći način sakupljanja adresa je pomoću robotskih skupljača (eng. harvester) – botova, odnosno programa koji na Webu traže e-mail adrese.

U posljednje vrijeme, kriminalci za širenje spama koriste botnet mreže. Riječ je o mrežama malverom zaraženih računala koje kriminalci uspijevaju anonimno kontrolirati. Korisnici zaraženih računala nisu ni svjesni da se njihova računala koriste za slanje spam poruka.



2.1: primjer e-mail spam poruke

Velike količine spam poruka gušile su promet ISP-ova, tako da su oni u svoju infrastrukturu ugradili mehanizme za njihovo filtriranje. Mnogi korisnici koriste vlastita programska rješenja, tako da je današnja detekcija spam poruka vrlo visoka. Zbog toga su kriminalci pribjegli i drugim metodama marketinga.

2.2 Malver

Što se malvera tiče, postoje različite vrste trojanskih konja koji na zaraženim računalima mijenjaju DNS zapise za popularne web pretraživače (naročito Google) te tako žrtve preusmjeravaju na krivotvorene servise vrlo sličnog izgleda. Takve replike servisa prilikom korisnikovih upita, uzimaju odgovore legitimnih servisa te ih modificiraju, odnosno na vrh liste dodaju rezultate (poveznice) koje vode prema ilegalnim web stranicama.

2.2: primjer rezultata pretrage koji sadrži maliciozni link (izvor: [4])

Druga vrsta malvera je TDSS obitelj [4] (prozvana prema imenu datoteke koju sadrži, a anagram vjerojatno dolazi od termina „Traffic Directing System“) koja zaražena računala preusmjerava na lažne anti-virusne programe ili jednostavno žrtvi servira reklame i linkove unutar web pretraga (slika) te ih time navodi na kupnju istih.

Osim osnovne funkcije, neke vrste malvera zaražena računala uvode u botnet mrežu.. Distribucija spama putem botnet mreža kriminalcima osigurava anonimnost i veliku fleksibilnost u pogledu upravljanja širenjem poruka.

2.3 Black-hat SEO

SEO je proces unaprjeđivanja vidljivosti, odnosno dostupnosti određene web stranice putem popularnih web tražilica (kao što su Google, Yahoo i Bing). Algoritmi web tražilica dodjeljuju određeni rejting web stranicama koji se ovom metodom pokušava povisiti. Time se osigurava veći broj korisnika jer web stranice s višim rejtingom se pojavljuju na vrhu listi kod pretraživanja.

Black-hat ili crni SEO koristi (od strane web pretraživača) nedozvoljene metode za povećanje rejtinga web stranica. Takve metode umanjuju efikasnost web tražilica, odnosno smanjuju kvalitetu pretraga za krajnjeg korisnika. Web stranice koje budu uočene da koriste takve tehnike se blokiraju ili im web tražilice postavljaju najniži mogući rejting. **Spamdexing** je zajednički naziv za skup različitih black SEO tehnika.

Jedna od najpopularnijih takvih tehnika je korištenje **doorway** (engl. kućni prag) web stranica čiji je sadržaj specifično kreiran i optimiziran za određene pojmove i fraze koji se pretražuju. Time se povećava rejting doorway stranice na web pretraživačima, odnosno ona će se naći više na popisu prilikom pretraživanja pojmova za koje je stranica optimizirana. Na takvim stranicama se nalaze poveznice (URL-ovi) ili JavaScript kod koje korisnike direktno upućuju na ranije spomenute ilegalne trgovine. Kao što im i samo ime kaže, doorway stranice nisu namijenjene posjećivanju od strane korisnika nego služe isključivo kao „kućni prag“ za glavne web stranice kriminalaca. Za pretraživanje popularnih pojmova (npr. Lady Gaga, smrt JFK-a itd.) pomoću kojih se doorway stranice optimiziraju koriste se alati koji automatiziraju taj proces, a neki odmah i sastavljaju gotove web stranice iz njih. Još jedna od tehnika je postavljanje posebnog skrivenog sadržaja kojeg vide samo botovi web pretraživača, dok se na stranicama nalazi posve drugačiji sadržaj. Sadržaj se prikriva na različite načine. Tekst se može sakriti ako se oboji jednako kao i pozadina ili mu se stavi vrlo mala veličina fonta, a isto tako se može i postaviti unutar HTML elemenata kao što su alt atributi, div atributi bez sadržaja, meta podaci i sl.

Cloacking je tehnika koja uključuje slanje različitog sadržaja spideru (botu) web tražilice od onog kojeg dobije posjetitelj. Ostvaruje se provjerom User-Agent HTTP zaglavlja ili IP adrese posjetitelja. Time se otkriva je li posjetitelj spider ili čovjek. Spideri služe web tražilicama za prikupljanje podataka o web stranicama, a ovom metodom „black-hat“ stranice dolaze na liste tražilica, što inače ne bi bio slučaj. Tehnika zatrpavanja poveznicama („link spamming“) koristi više web stranica koje upućuju jedna na drugu u svrhu povišenja rejtinga jer algoritmi tražilica (npr. Google PageRank) daju viši rejting onim stranicama na koje upućuje veći broj drugih. Isto se postiže i spam porukama, koje sadrže poveznice, na komentarima popularnih blogova.
U posljednjih nekoliko godina, efekt korištenja navedenih tehnika je znatno umanjen nadogradnjama algoritama za pretraživanjem koje koriste web tražilice.

3 Vrste partnerki

3.1 Canadian Pharmacy

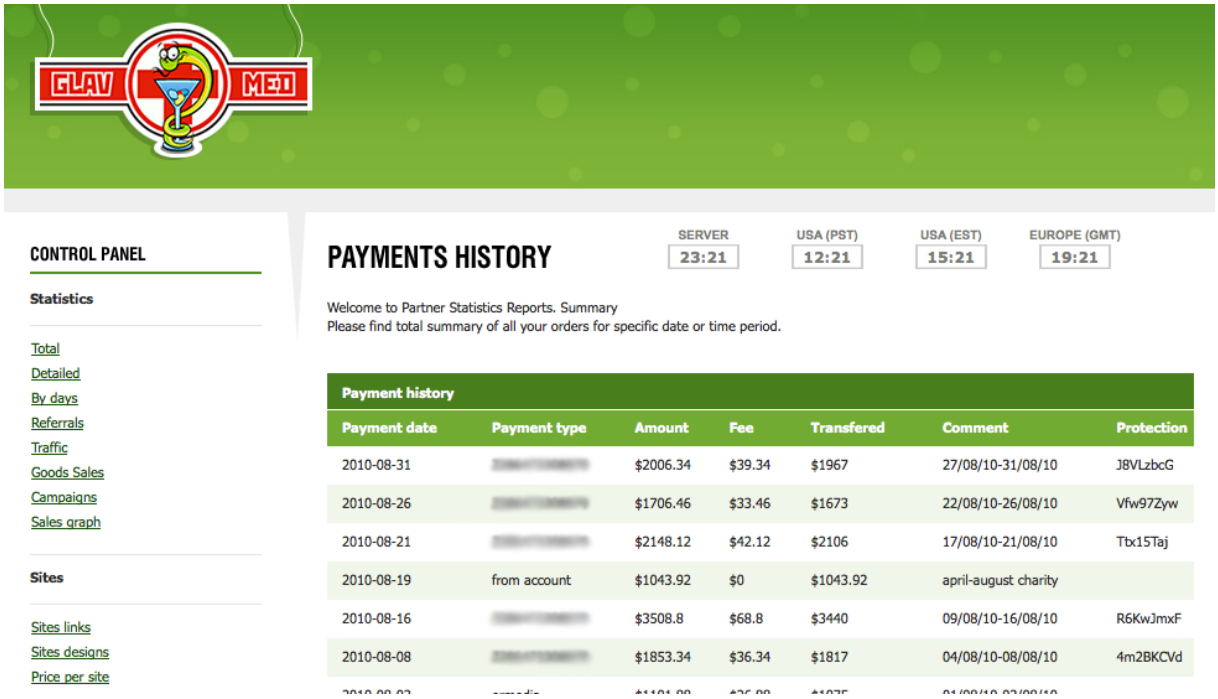
Web trgovine s farmaceutskim proizvodima najčešći je oblik „poslovanja“ partnerki. Najveća i najpoznatija partnerka je GlavMed („glav“ je skraćeno od glavna). GlavMed je javno dostupan, ali za registraciju je potrebno dobiti pozivnicu od nekog drugog člana mreže. Najpoznatiji „brand“ mreže je tzv. „Canadian Pharmacy“ (kanadska farmaceutika), dobro poznata po ogromnoj reklami putem masovnog spama.

3.1: početna stranica Glavmeda (izvor: [5])

GlavMed na svojim javnim web stranicama zagovara anti-spam politiku i legalni SEO. Međutim, pretragom telefonskog broja korisničke službe putem Googlea, vidi se da se isti broj pojavljuje na više od 100 tisuća različitih web trgovina. Također je otkriveno kako se na tim stranicama koristi isti PHP backend sustav kao i na GlavMedu. Kriminalni poslovni model je sljedeći. Korisnici, odnosno partneri GlavMeda administriraju partnerske web stranice i zaduženi su za generiranje što većeg Internet prometa na svojim stranicama koje u biti sve vode prema istoj trgovini, odnosno cilj im je zaprimiti što veći broj narudžbi. Zauzvrat od Glavmeda dobivaju određeni postotak zarade (35-40%) od prodaje lažnih farmaceutskih proizvoda. Partnerima takav postotak omogućuje vrlo dobru zaradu čak i uz samo nekoliko kupnji dnevno.

Putem javnog portala partneri pristupaju korisničkom dijelu GlavMeda na kojem mogu vidjeti statistiku posjećenosti svojih (partnerskih) web stranica i zaradu. Administratori partnerskih web stranica imaju opciju preuzimanja dviju inačica web trgovina s GlavMeda ili mogu jednostavno samo preusmjeravati promet na skup domena kojima upravlja GlavMed. Svaka partnerska trgovina posjeduje u pozadini sučelje koje GlavMedu omogućuje obradu narudžbi i nadzor nad statistikom. Na glavnoj stranici GlavMeda nalazi

se i forum na kojem partneri razmjenjuju ideje i dobivaju tehničku pomoć. Iako je GlavMed najstarija i najveća mreže ove vrste postoje još mnoge druge kao što su Stimul-cash.com, Rx-partners, Rxcash.biz, Evapharmacy, Rx-Signup.com i DrugRevenue [2].



3.2: Glavmed i povijest novčanih uplata partnerima (izvor: [3])

SpamIt mreža, koja je zatvorena 1. listopada 2010., bila je zatvoreniji dio GlavMed mreže, a njezini navodni članovi upravljaju i zloglasnim botnet mrežama kao što su Storm, Waladec i Conficker. Međutim, voditelji mreže su je odlučili zatvoriti nakon što je privukla veliku pažnju od strane nadležnih institucija. Po nekim navodima, u mrežu su se infiltrirali ruski sigurnosni istražitelji, a sigurno je znatan utjecaj imala tadašnja nova anti-spam kampanja Ruskog udruženja za elektroničku komunikaciju (RAEC) [1]. Sigurnosni istraživač Krebs je u veljači 2011. na svojem blogu objavio [3] informacije o poslovanju SpamIt-a dobivene iz anonimnog izvora koji je imao pristup cijeloj pozadinskoj bazi podataka navedene mreže. Baza je sadržavala kontakt i povjerljive podatke od ukupno 800 tisuća kupaca farmaceutskih proizvoda od kojih je ukupno zaprimljeno 1.5 milijuna narudžbi, a sve u razdoblju od svibnja 2007. do lipnja 2010. Navedeni podaci su također otkrili kako je SpamIt imao čak 2500 partnera, zaduženih za marketing i prodaju. Statistika iz baze podataka pokazala je kako je svaki od prvih osam partnera po zaradi, zaradio više od milijun američkih dolara. Procijenjeno je kako je ukupan ostvareni prihod SpamIt-a iznosio barem 150 milijuna američkih dolara. Većina partnera isplaćivana je putem ruskog servisa Webmoney, sličnog PayPalu, osim što su transakcije nepovratne, dok je dio plaćen putem servisa ePassporte, koji je zatvoren u rujnu 2010. nakon optužbi za prijevaru i ilegalno korištenje sredstava s korisničkih računa.

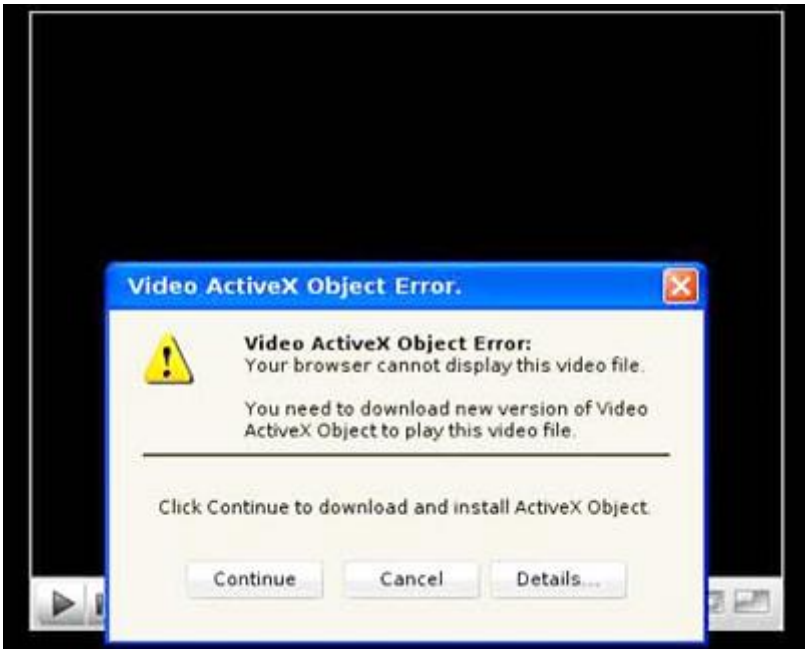
3.2 Soft-partnerka

Socijalni inženjering vezan uz zastrašivanje korisnika i navođenje na preuzimanje (malicioznih) lažnih antivirusnih programa, tzv. scareware-a je trend u posljednjih nekoliko godina. Uz sveprisutni socijalni inženjering, napadači koriste i ranjivosti u softveru kao što

su na primjer web preglednici i čitači PDF dokumenata. Koriste opću zabrinutost i strah od malvera kako bi naveli korisnike na instalaciju scareware-a. Nakon instalacije, malver žrtve zatrpava upozorenjima kako im je računalo zaraženo i traži novčanu uplatu za kupnju lažnog softvera koji će te „viruse“ ukloniti. Ono što je manje poznato u vezi scareware-a je da ga kriminalci ostvaruju ovaj oblik zarade također uz pomoć umreženosti partnerkama.

3.3: PM Software - jedna od partnerki koja je bila zadužena za distribuciju scarewarea (izvor: [4])

U ovom slučaju partneri ostvaruju prihod na temelju broja ostvarenih instalacija malvera (tzv. model „pay per install“). Partnerima je dakle uloga žrtve navesti na instalaciju malvera koristeći neku od mnogih metoda. U tu svrhu partneri koriste različite oblike promotivnih materijala u obliku HTML i skriptnog koda, zaduženog za navođenje korisnika na klikanje, odnosno instalaciju. Često se koristi navođenje žrtvi na instalaciju lažnih video codeca stoga se ova vrsta partnerke naziva i „codec-partnerka“.



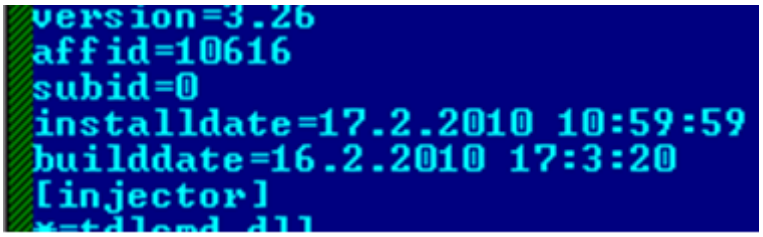
3.4: poruka koja navodi potencijalnu žrtvu na instalaciju lažnog codeca

Drugi oblik popularni oblik su različite varijacije kopija popularnih pornografskih web stranica (poput PornTube-a). Ova vrsta partnerke je nešto zatvorenijeg tipa i da bi se postalo partnerom potrebno je imati određenu reputaciju, no postoje i nešto otvorenije kao što je Buckster.ru. Dva najpoznatija lažna antivirusna programa navedene organizacije su WinXdefender i VirusDoctor. Druga vrlo popularna partnerka je RefreshStats koja je nešto zatvorenija [2].

Važno je napomenuti da je scareware ovog tipa pogađao ne samo Windows računala, nego i ona s operacijskim sustavom MacOS. U svibnju 2011. su se pojavile različite inačice lažnih antivirusnih alata koje su pogađale MacOS [6]. Malver se pojavio u nekoliko oblika pod različitim imenima, od kojih je najpoznatiji „MacDefender" koji se pojavio prvi. Scareware je tražio od žrtve uplatu od 60 do 80 američkih dolara kako bi „uklonio" viruse i trojanske konje s njegovog računala te kako bi ga prestao zatrpavati silnim upozorenjima.

3.5: primjer poruke koje prikazuje scareware

Kako bi partner, koji je naveo korisnika na instalaciju malvera, mogao biti novčano isplaćen, malver pohranjuje podatke o njemu. Riječ je o je tzv. aff (affiliate) ID koji identificira partnera[4]. Obično je to brojčana vrijednost koja je pohranjena u konfiguracijskoj datoteci malvera. AffID se šalje administratorskoj kontrolnoj ploči na webu, kao i nekoliko drugih podataka kao što su IP adresa, i OS zaraženog računala te GUID (jedinstvena oznaka zaraženog računala).



3.6: affID unutar konfiguracijske datoteke malvera (izvor: [4])

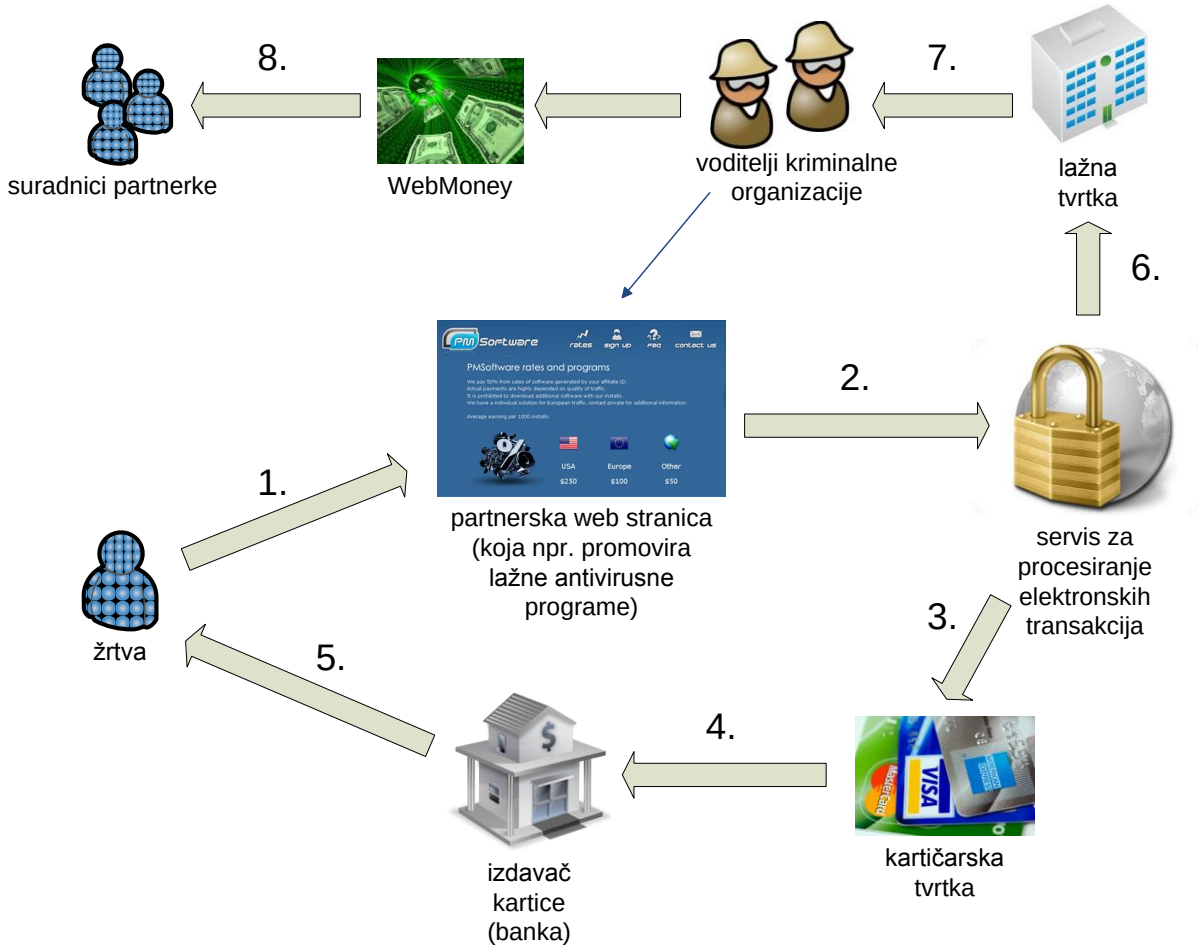
Samosseiko [2] je istražio i soft-partnerku Topsale2.ru koja je na glavnoj stranici bez ustručavanja isticala različite informacije. Prihvaćan je isključivo promet iz SAD-a, Kanade i Australije, e partneri bi po prodanom softveru zarađivali 25 američkih dolara. S obzirom da je stranica navela i zaradu od 100-250 dolara po 1000 preuzetih scareware alata, može se zaključiti kako maksimalno 10 od 1000 korisnika zaista i plati za lažni softver. Promotivni materijali koje nudi ova partnerka uključuju dinamičke web stranice koje obmanjuju korisnika kako skeniraju njegovo računalo i kako su pronađeni virusi, lažne codece te tri različite izvršne (EXE) datoteke, od kojih je jedna namijenjena uključivanju računala žrtve u botnet mrežu. Tijekom 2008. Sophos je nadgledao više desetaka soft-partnerka stranica od kojih svaka održava svoj skup softvera i promotivnih materijala, stoga ne čudi količina scareware-a koje se pojavila na Internetu u zadnjih nekoliko godina.

4 Organizacija

4.1 Model naplate

Kako bi mogli doći do novčanih sredstava, platiti svoje suradnike iz partnerke, a pritom prikriti svoj identitet i svoje kriminalne aktivnosti, vođe kriminalnih skupina koriste složen sustav naplate. Sustavi različitih vrsti partnerki, odnosno organizacija imaju jednaku zajedničku strukturu, koja se može promatrati iz analize [7] partnerki koje se bave prodajom lažnih antivirusnih programa (scarewarea). Sustav je prikazan na slici 4.1.

Cijeli proces novčane transakcije započinje kad žrtva putem web stranice ostvari kupnju nekog lažnog proizvoda, odnosno pošalje podatke o svojoj kreditnoj kartici (korak 1 na slici). Prodavatelj podatke o kartici prosljeđuje servisu za procesiranje elektronskih transakcija (korak 2). Jedan od često korištenih takvih servisa je ChronoPay, najveći servis takve vrste u Rusiji [8]. Nakon toga, servis mora proslijediti podatke jednoj od velikih kartičarskoj tvrtki (korak 3), koja potom traži autorizaciju od izdavača njene kreditne kartice (4). Ako se izdavač transakciju odobrio, izvršava se naplata (5) i kartičarska tvrtka obavještava servis za procesiranje o uspješnoj transakciji. Servis za procesiranje periodično (obično svaka dva tjedna ili mjesec dana) vrši uplate na bankovne račune lažnih tvrtki koje su otvorili voditelji kriminalne organizacije (6). Oni podižu taj novac (7) i koriste ga za plaćanje provizije svojim suradnicima (administratorima partnerskih stranica itd.).



4.1: tipičan model naplate kod partnerki

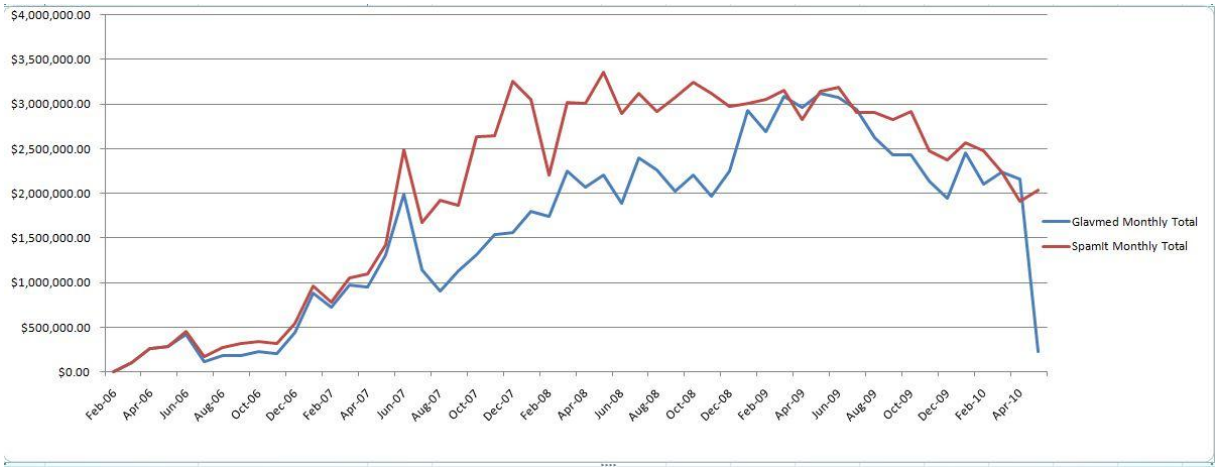
Manji servisi, odnosno tvrtke za procesiranje, često usko surađuju s kriminalcima i za to bivaju plaćeni određenim postotkom od zarade. Većim servisima, koji većinu prometa ostvaruju legalnim poslovanjem (poput ChronoPaya ili ePassportea), ilegalne transakcije čine samo manji dio zarade kojega se ne žele odreći ili nemaju volju poduzeti potrebne mjere za blokadu takvih transakcija. Poznato je kako je servis ePassporte ostao bez prava za korištenje VISA kartica zbog velike količine transakcije vezanih uz prijevaru [7]. U slučaju velikog broja prijava prijevare od strane korisnika (korisniku se pritom vraća novac, tzv. chargeback) prema izdavaču kartice, servis za procesiranje može odlučiti zabraniti sve transakcije s tvrtkom u pitanju. Zbog toga su kriminalci redovito pratili broj žalbi i, zanimljivo, vraćali novac određenom broju korisnika. Istraživanje [7] pokazalo je kako postoji korelacija između broja žalbi i broja povrata novca. Drugim riječima, u slučaju kada bi se povećao broj žalbi, kriminalci bi češće vraćali novac natrag, u dovoljno mjeri da ih servis za procesiranje ne blokira. Također, kako bi smanjili broj žalbi, kriminalci često mijenjaju imena svojih proizvoda. Razlog tome je što korisnike na žalbu potiču drugi korisnici koji se žale na isti proizvod na različitim internetskim forumima i sl. na koje žrtva nailazi putem web tražilica.

Naknade suradnicima partnerke obično se ostvaruju pomoću servisa WebMoney. Razlog tome je što su sve transakcije na navedenom servisu anonimne i nepovratne, a naknada koju naplaćuje iznosi samo 0.8%. Također, velik broj gradova, posebice u istočnoj Europi, nudi konverziju WebMoney novca u lokalnu valutu.

4.2 Novčana zarada

Prema [10] više od polovice novčanih transakcija kod kupnje lažnih farmaceutskih proizvoda naplaćeno je putem kreditnih i debitnih kartica koje su izdale najvećih sedam banaka-izdavača kartica iz SAD-a. Istraživanje [9] je pokazalo kako su tri financijske tvrtke (iz Azerbajdžana, Danske i karipskog otočja Nevis) obrađivale čak 95% transakcija kreditnim karticama. To pokazuje da su banke mjesto gdje se može zaustaviti kriminalna aktivnost. Ako banke blokiraju uplate prema manjem broju drugih financijskih tvrtki, cijeli kriminalni sustav bi pretrpio snažan udar.

Prema podacima o novčanom poslovanju iz Glavmedove ukradene baze podataka, koja je dostavljena web portalu KrebsOnSecurity [10], vidljivo je o kakvim je brojkama riječ. Grafikon prikazuje mjesečnu zaradu GlavMeda i SpamIta od 2006. do 2010. godine:



Mjesečna zarada svake od organizacija u prosjeku je iznosila više od 2 milijuna američkih dolara. Zbrojeno, sveukupna zarada tijekom te četiri godine iznosila je preko 70 milijuna dolara. Vjerojatno je riječ o samo dijelu sveukupne zarade.

5 Zaključak

Kriminalni marketing putem Interneta, kao milijunski biznis, privlači veliki broj ljudi zbog mogućnosti vrlo dobre zarade „od doma“. S druge strane, Internet omogućuje anonimnost, odnosno sigurnost od kaznenog progona voditeljima ovakvih organizacija. Oni često surađuju s ISP-ovima kojima je poznata ilegalna aktivnost njihovim klijenata, ali ih to ne brine ili država u kojoj se nalaze nema potrebnu administraciju i zakone za rješavanje ovog problema.

U posljednjih nekoliko godina, ovakva vrsta kriminala je glavna pokretačka snaga koja stoji iza spama, malvera i mnogih drugih zloupotreba na Internetu. To je s vremenom uzrokovalo odgovor od strane računalnih sigurnosnih stručnjaka, njihovih tvrtki i državnih institucija koje sve više surađuju na globalnoj razini. To se najbolje vidi u slučajevima gašenja SpamIt-a i nekoliko botnet mreža, odnosno ISP-ova koji su stajali iza njih. Time je podzemlju zadan jak udarac jer im se time mnogostruko dižu novčani izdaci koje je potrebno uložiti u prikrivanje svojih aktivnosti i identiteta.

Nadalje, obzirom kako kriminalci za svoje transakcije moraju koristiti banke, a istraživanja su pokazala kako one imaju mogućnost lako otkriti nelegalne transakcije, blokiranjem određenih klijenata, može se posve onemogućiti tok nelegalnog novca. Kriminalcima je potrebno određeno vrijeme za otvaranje novih tvrtki i računa, tako da suradnjom s nadležnim tijelima, banke imaju mogućnost pravodobno blokirati sav nelegalni promet.

Uz prijekopotrebnu globalnu suradnju relevantnih tijela na ovom području, potrebne su i nove zakonske regulative. Time se na vrijeme može onemogućiti ilegalan rad klijenata ISP-ova koji to dopuštaju. Upravo je sporost zbog administracije i nedovoljna suradnja razlog neučinkovite borbe protiv ovakve vrste kriminala te je tu još potrebno ostvariti napredak.

6 Literatura i reference

1. B. Krebs: Spam Affiliate Program Spamit.com to Close, http://krebsonsecurity.com/2010/09/spam-affialite-program-spamit-com-to-close , objavljeno 27.9.2010.
2. Dmitry Samosseiko: The Partnerka - What Is It, and Why Should You Care, SophosLabs Canada, rujan 2009.
3. B. Krebs: SpamIt, GlavMed Pharmacy Networks Exposed, http://krebsonsecurity.com/2011/02/spamit-glavmed-pharmacy-networks-exposed/ , veljača 2010.
4. Golovanov, Rusakov - TDSS, Securelist, http://www.securelist.com/en/analysis/204792131/TDSS , 5.8.2010.
5. Spamtrackers.eu, http://spamtrackers.eu/wiki/index.php/Glavmed
6. G. Keizer: Mac scareware gang and Apple trade blows yet again, MacWorld, http://www.macworld.co.uk/macsoftware/news/index.cfm?newsid=3284106 , 6.6.2011.
7. B. Stone-Gross, R. Abman, R. A. Kemmerer, C. Kruegel, D. G. Steigerwald, G. Vigna: The Underground Economy of Fake Antivirus Software, Universitiy of California, Santa Barbara, lipanj 2011.
8. B. Krebs: ChronoPay's Scareware Diaries, http://krebsonsecurity.com/2011/03/chronopays-scareware-diaries/ , 3.3.2011.
9. K. Levchenko i dr.: Click Trajectories: End-to-End Analysis of the Spam Value Chain, preuzeto sa http://cseweb.ucsd.edu/~savage/papers/Oakland11.pdf , svibanj 2011.
10. B. Krebs: Banks Hold Key to Killing Rogue Pharmacies, http://krebsonsecurity.com/2011/06/banks-hold-key-to-killing-rogue-pharmacies/ , lipanj 2011.