CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Online ucjene

CCERT-PUBDOC-2009-06-268

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Tvrtke sve češće koriste internetsku mrežu za reklamiranje svojih proizvoda i usluga. Budući da tvrtke postavljaju informacije na Internet, korisnici mogu brzo, jednostavno i učinkovito doći do podataka. Često se uvodi i mogućnost narudžbe i kupnje proizvoda, što daje dodatne prednosti Internet marketingu. Ipak, ovakvo rukovanje informacijama donosi i razne sigurnosne probleme. Osim problema koje donosi rukovanje privatnim podacima korisnika, tvrtke se sve češće susreću sa internetskim prevarama.

Jedna od osnovnih napadačkih tehnika koji se koriste u *online* prevarama je stvaranje zlonamjernih programa te njihovo podmetanje korisnicima. Ovaj pojam uključuje sve oblike programa kojima je cilj krađa podataka te uništavanje ili oštećivanje računalnog sustava. Kako bi izvršili *online* prevaru, napadači se obično koriste s dvije vrste zlonamjernih programa: *scareware* i *ransomware*.

Prva skupina spomenutih programa služi za zastrašivanje korisnika kako bi ga se nagovorilo na kupnju nekog lažnog antivirusnog alata ili drugog proizvoda koji se koristi kao zaštita operacijskog sustava i korisničkih podataka. Pri tome se koriste lažne poruke o detekciji raznih zlonamjernih programa na računalu korisnika prikazanih u prozorima koji se pojavljuju prilikom posjećivanja neke web stranice (eng. pop-up ad). Druga skupina programa, zvanih *ransomware*, je ozbiljniji oblik zlonamjernih programa korištenog za *online* ucjene u smislu da donosi više štete korisnicima. Radi se o zlonamjernom kodu koji se koristi raznim tehnikama kako bi zaključao korisničko računalo ili kriptirao važne datoteke na sustavu. Sljedeći korak uključuje ostavljanje poruke korisniku u obliku tekstualne datoteke ili prozora s uputama o dobivanju ključa. Napadači obično zahtijevaju isplatu određenih novčanih iznosa za kriptografske ključeve ili lozinke za otključavanje.

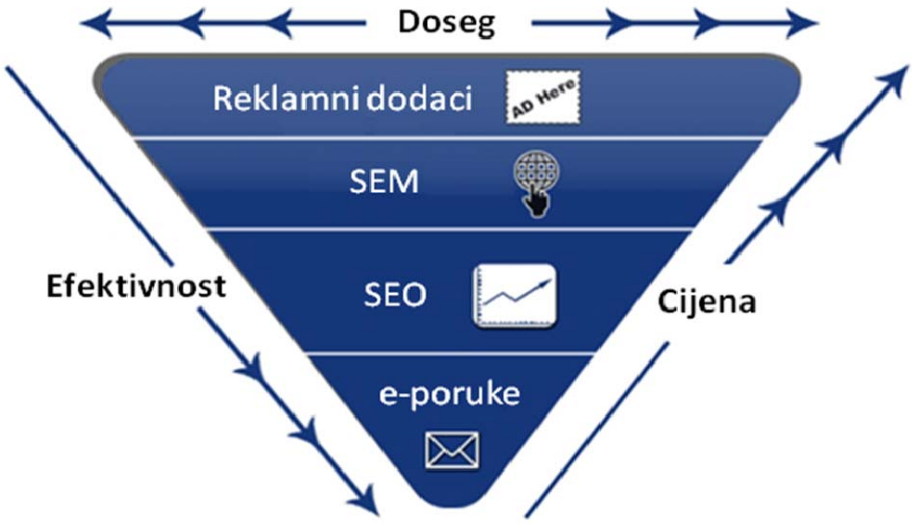
Iako se mnoge sigurnosne organizacije (npr. Kaspersky Lab) bore protiv ovakvih programa, posao im otežavaju napadači koji počinju s uporabom sve složenijih algoritama. Vjeruje se kako će napadači u skorijoj budućnosti stvoriti dovoljno sofisticiran alat čije lozinke sigurnosni stručnjaci neće moći dekriptirati. Kako bi se krajnji korisnici zaštitili, moraju se pridržavati osnovnih sigurnosnih mjera. U to se ubraja uporaba antivirusnih programa, vatrozida te redovito osvježavanje inačica operacijskog sustava i preglednika, kao i drugih programa. Osim tih osnovnih metoda zaštite, korisnicima se savjetuje primjena alata za blokiranje *pop-up* prozora, kao i izrada sigurnosnih kopija važnih podataka.

2. Internet marketing

Pojam „Internet marketing“ označava prodavanje proizvoda ili usluga preko internetske mreže. Često se koriste i pojmovi *„i-marketing“*, *„web marketing“*, *„online marketing“* ili *„eMarketing“*.

Pojava Interneta donijela je mnogo jedinstvenih prednosti procesu prodavanja, od kojih je jedna niža cijena distribucije informacija i proizvoda globalnom tržištu. Interaktivna priroda Internet marketinga, u smislu pružanja trenutnog odgovora na ponudu, predstavlja jedinstvenu kvalitetu trgovanja. Ponekad se smatra da Internet marketing ima širi raspon jer se ne odnosi samo na digitalne medije (poput poruka elektroničke pošte) nego uključuje i upravljanje digitalnim podacima (održavanje sigurnosti i pouzdanosti korisničkih informacija) te ECRM (eng. electronic customer relationship management) sustav (svi oblici upravljanja vezama s korisnicima preko informacijskih tehnologija). Povezuje kreativne i tehničke aspekte Interneta uključujući dizajn, razvoj, oglašavanje i prodaju.

Internet marketing također se odnosi na okupljanje korisnika oko različitih tvrtki kroz SEM (eng. search engine marketing), SEO (eng. search engine optimization), reklamne natpise (banner) ili posebne oglašavajuće web stranice te poruke elektroničke pošte. SEM marketing je oblik Internet marketinga koji se temelji na promoviranju web stranica povećavanjem njihove vidljivosti u rezultatima pretrage tražilicom. SEO optimiziranje označava povećavanje volumena prometa neke stranice na način da se stranica prikaže među prvim rezultatima pretrage. *Slika 1* prikazuje odnos između dosega, efektivnosti i cijene prethodno navedenih načina marketinga.



Slika 1 Utjecaj *online* reklamiranja

Internet marketing je povezan s nekoliko modela poslovanja (okruženja za stvaranje ekonomskih, socijalnih i nekih drugih oblika vrijednosti):

- prodaja i kupnja proizvoda i usluga preko elektroničkog sustava (eng. e-commerce) – dobra se prodaju izravno kupcima,
- oglašavanje – prodaja reklamnog prostora,
- udruženi marketing – proces u kojem proizvod ili uslugu jedna osoba prodaje drugom aktivnom prodavaču za dijeljeni profit pri čemu vlasnik proizvoda kreira potrebni marketinški materijal. Primjer je projekt ODP (eng Open Directory Project), popis poveznica na web stranice grupiranih u više kategorija koji održava skupina volontera.

Postoji više pristupa u definiranju Internet marketinga nekog poduzeća:

1. Jedan-na-jedan pristup (eng. one-to-one approach) – ciljani korisnik obično pregledava Internet stranicu pa izravno susreće marketinške poruke. Koristi se u reklamiranju temeljenom na ključnim riječima koje korisnik upisuje u tražilicu.

2. Apeliranje na posebne interese (eng. appeal to specific interests) – marketing apelira na posebno ponašanje na Internetu prema dobnim grupama, spolu i drugim općim faktorima.
3. Geo marketing – metode određivanja geografske lokacije (država, regija, grad i sl.) posjetitelja web stranice preko programa koji određuje lokaciju korisnika (npr. preko IP adrese) te pružanje različitog sadržaja ovisno o lokaciji posjetitelja. Geo marketing se može podijeliti u dvije osnovne kategorije:
    a. Različit sadržaj po izboru (eng. different content by choice) – tipičan primjer pružanja različitog sadržaja po izboru je web stranica FedEX gdje korisnici mogu odrediti svoju lokaciju kako bi dobili odgovarajući sadržaj.
    b. Automatsko pružanje različitog sadržaja (eng. automated different content) – pružanje sadržaja temelji se na lokaciji ili drugim osobnim podacima korisnika.

2.1. Online reklamiranje

Online reklamiranje je oblik promoviranja koji koriste tvrtke na Internetu za isticanje potrebe o uporabi marketinških poruka kako bi se privukli kupci. Jedna velika dobit *online* reklamiranja je trenutačna objava informacija i sadržaja koju ne ograničava geografski položaj ili vrijeme. Druga prednost je učinkovitost ulaganja, što označava da se isplati ulaganje u *online* reklamiranje zbog brzog širenja informacija, jeftinijeg oglašavanja te privlačenja većeg broja kupaca.

Neki od oblika *online* reklamiranja uključuju:

- reklamiranje porukama elektroničke pošte – oblik izravnog reklamiranja gdje se koriste poruke elektroničke pošte kao sredstvo prosljeđivanja poruka ciljanim grupama. Pojam se obično koristi za:
    - slanje poruka elektroničke pošte s ciljem održavanja veza sa trenutnim ili prijašnjim klijentima,
    - slanje poruka elektroničke pošte za prikupljanje novih korisnika,
    - slanje poruka elektroničke pošte za ubrzano obavještavanje trenutnih korisnika o novim proizvodima i/ili uslugama.
- kontekstno reklamiranje – mnoge web stranice reklame prikazuju preko grafičkih ili samo tekstualnih dodataka koji odgovaraju ključnim riječima u tražilici ili sadržaju web stranice na kojima se nalaze. Obično imaju veliku šansu za privlačenje korisnika jer sadrže sličan sadržaj kakav korisnici traže. Novija tehnika ovakvog oglašavanja je umetanje sponzoriranih poveznica (eng. hyperlinks) u članke.
- reklamiranje prema ponašanju korisnika – reklamiranje se usmjerava prema ponašanju korisnika (npr. web stranicama koje je pregledao u prošlosti) ili analiziranjem kolačića (eng. cookies) pohranjenih u korisničkim računalima.
- reklamiranje dodacima (Slika 2) – metode reklamiranja koje bi se mogle smatrati neetičnim ili ilegalnim, a uključuju vanjske aplikacije koje pokreću dodatne prozore s reklamama (eng. pop-ups) te umetanje oglasa. Često su povezane s programom koji je instaliran na računalu za skupljanje informacija o korisniku (eng. spyware) ili programom koji automatski prikazuje ili preuzima reklame tijekom korištenja aplikacije (eng. adware). Takve aplikacije su skrivene izvedbom jednostavne radnje poput prikaza vremena. Obično su dizajnirane na način da ih je teško ukloniti sa korisničkog računala.

Slika 2 *Online* reklamiranje porukama

Osnovni načini naplate *online* reklamiranja su:

- CPM (eng. Cost Per Mille) ili CPI (eng. Cost Per Impression) – tvrtke plaćaju za izlaganje svojih poruka posebnoj grupi korisnika. Izraz „Per Mille“ označava tisuću prikaza krajnjem korisniku s tim da se određeni prikazi ne računaju (npr. ponovno učitavanje).
- CVP (eng. Cost Per Visitor ili Cost per View in the case of Pop Ups and Unders) – tvrtke plaćaju za usmjeravanje korisnika na određenu web stranicu.
- CPC (eng. Cost Per Click) – tvrtke plaćaju za svaki klik na poveznicu i preusmjeravanje na svoju web stranicu, a ne za sam oglas.
- CPA (eng. Cost Per Action ili Cost Per Acquisition) – temelji se na izvedbi i najčešće se koristi u dijeljenom marketingu. Oglašavač preuzima odgovornost o reklami, a tvrtka plaća samo za korisnike koji obave kupnju proizvoda/usluge.

2.2. Prednosti i ograničenja

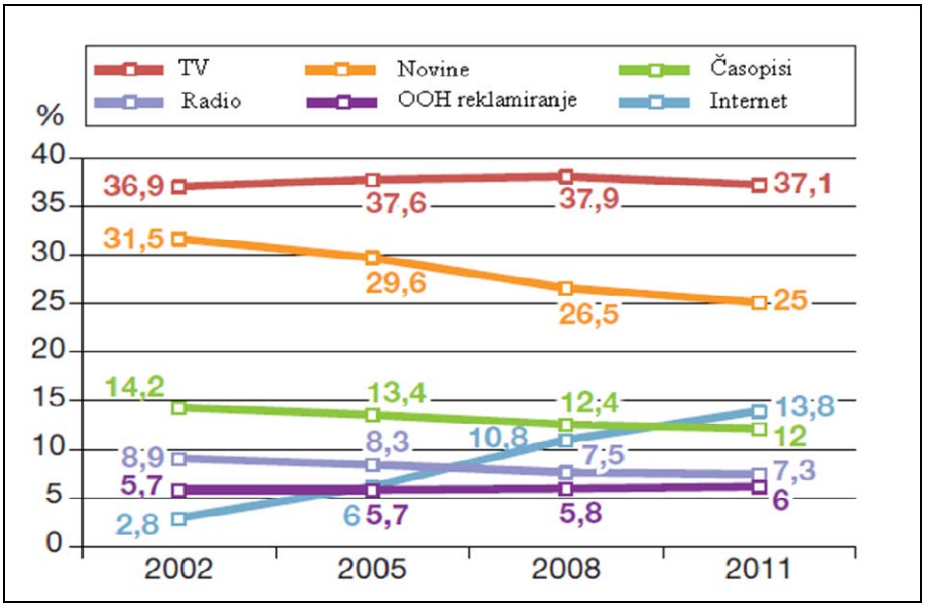
Internet marketing je relativno jeftin način reklamiranja u usporedbi s drugim načinima (npr. reklamiranje putem radija ili televizije). Zahvaljujući njemu tvrtke mogu brzo i jeftino kontaktirati velik broj korisnika te ponuditi proizvode ili usluge pod vlastitim uvjetima. Osim toga, korisnicima se većinom omogućuje jednostavno kontaktiranje proizvođača i narudžba željenog proizvoda.

Također, Internet marketing ima prednost jednostavnog i jeftinog mjerenja statistike. Tvrtke koje postavljaju oglase mogu se poslužiti različitim tehnikama prilikom praćenja korisnika za potrebe izrade statistike:

- plati po izdanju (eng. pay per impression),
- plati po kliku (eng. pay per click),
- plati po reprodukciji (eng. pay per play),
- plati po akciji (eng. pay per action).

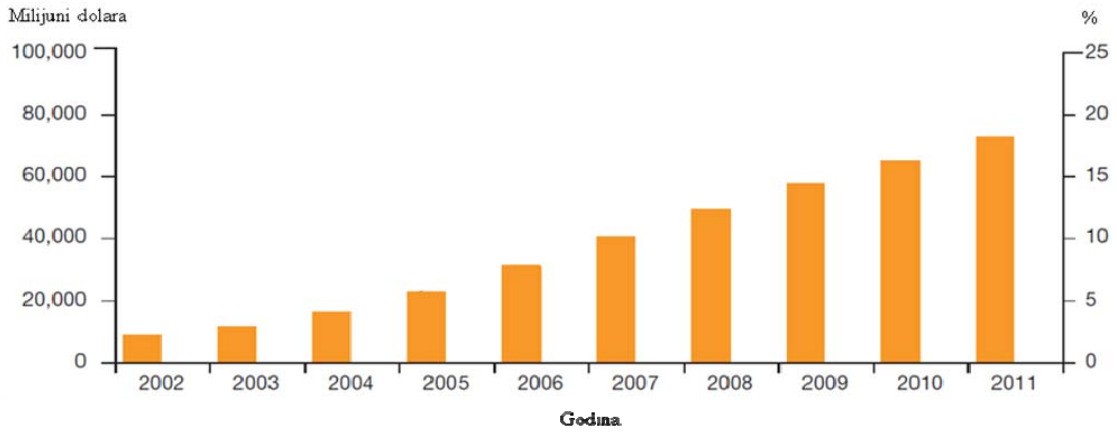
Navedenim postupcima može se odrediti čije su ponude ili poruke primamljivije korisnicima.

Od 2007.g. Internet marketing raste brže od drugih načina prodavanja i oglašavanja zahvaljujući cjelokupnoj učinkovitosti. Prema izvješću „World Media Digital Trends 2007“ (http://www.wan-press.org/worlddigitalmediatrends/download.php?type=pdf&file_name=Summary_wdmt_2008) globalno reklamiranje naglo je poraslo nakon 2002. godine, a očekuje se i daljnji rast. Iako se i dalje kao osnovna sredstva reklamiranja koriste mediji poput televizije i novina, primjećuje se znatan rast Internet marketinga. Najslabiji rast pokazuje OOH (eng. out-of-home) reklamiranje koje se temelji na utjecaju na korisnika dok je izvan kuće (primjer su reklame na plakatima uz prometnice). Odnos udjela i rasta reklamiranja po sektorima u razdoblju od 2002 . do 2011. godine prikazuje Slika 3.



Slika 3 Raspodjela i rast globalnog oglašavanja po sektorima

Porast troškova Internet marketinga izdvojen je na **Error! Reference source not found.**, gdje se također primjećuje rast ulaganja u ovu vrstu reklamiranja.



Slika 4 Rast ulaganja u Internet marketing

Ipak, Internet marketing zahtjeva od korisnika uporabu novijih tehnologija. Jedno od mogućih ograničenja su i Internet veze malih brzina (spajanje na Internet preko *dial-up* veza ili mobilnih uređaja) što uzrokuje kašnjenje u prikazu sadržaja.

Također, kupci često imaju predrasude prema proizvodu koji ne mogu dodirnuti ili isprobati. Ipak, sve je češća praksa povratka proizvoda prodavaču ako korisnik nije zadovoljan.

2.3. Sigurnosni problemi

Sigurnost informacija je jednako važna tvrtkama i korisnicima uključenim u *online* poslovanje. Mnogi korisnici izbjegavaju trgovanje preko Interneta jer ne vjeruju da će njihovi osobni podaci ostati zaštićeni. Osnovna metoda implementiranja politike privatnosti je kriptiranje podataka, tj. proces transformiranja podataka uporabom nekog algoritma kako ne bi bili čitljivi korisnicima bez posebnih informacija (kriptografskog ključa).

Nedavno je otkriveno da nekoliko tvrtki koje obavljaju *online* poslovanje prodaju informacije o svojim klijentima. Nekoliko od tih tvrtki nude garanciju na web stranicama o privatnosti korisničkih podataka. Također, neke od navedenih tvrtki daju korisnicima mogućnost uklanjanja privatnih podataka iz baze podataka (eng. opting out). Incidenti povezani uz krađu privatnih podataka putem neke „tuđe" web stranice povećavaju nepovjerenje prema istima.

Još jedan veliki sigurnosni problem predstavlja potreba za povjerenjem koju korisnici iskazuju prilikom narudžbe proizvoda ili usluga. Trgovci se često oslanjaju na široko raširene i poznate web stranice (npr. Amazon.com, eBay i sl.).

Prevare na klik su tip internetskih prevara koji se često pojavljuju u *online* reklamiranju. Očituju se kada osoba ili program oponaša legitimnog korisnika web preglednika klikom na reklamni dodatak s ciljem naplate posjećene poveznice.

Osim opisanih, postoje još mnoge sigurnosne prijetnje u trgovanju preko Interneta. Također, sve se češće pojavljuju prevare u kojim se korisnike navodi na kupnju određenog proizvoda (većinom računalnog programa) uz upozorenja o potrebi zaštite računala od nekog zlonamjernog programa. Kao jedan od ozbiljnijih oblika internetskih prevara javljaju se *online* ucjene. Najčešće uključuju preuzimanje prava pristupa ili pregleda određenih korisnikovih datoteka te zahtijevanje isplate određene sume novca za povrat istih. Budući da uklanjanje takvih zlonamjernih programa zahtjeva puno vremena i znanja, korisnici su prisiljeni plaćati tražene novčane iznose kako bi dobili zaključane podatke. Mnogi korisnici nisu upoznati s prijetnjama koje donose programi namijenjeni *online* ucjenama. U nastavku dokumenta moguće je pročitati više o zlonamjernim programima i načinu zaštite.

3. Zlonamjerni programi za online ucjene

Zlonamjerni programi (eng. malware) su programi dizajnirani kako bi oštetili računalne sustave bez znanja korisnika. Uključuju računalne viruse, crve, trojanske konje te ostale slične programe. Potrebno je razlikovati zlonamjerne programe od legitimnih programa koji sadrže ozbiljne ranjivosti. Zlonamjerni programi su stvoreni s ciljem nanošenja štete računalima korisnika. Legitimni programi s ranjivostima su stvoreni kako bi imali neku korisnu namjenu, ali zbog pogrešaka u implementaciji sadrže sigurnosne ranjivosti.

Mnogi od prvih zlonamjernih programa, uključujući „Internet crv" (eng. Morris worm/Internet worm), stvoreni su kao pokus te nisu imali zlonamjernu svrhu. Ipak, svakim se danom pojavljuje sve više programa koji kao cilj imaju uništenje podataka ili računalnog sustava. Također, nakon povećanja broja korisnika s širokopojasnim pristupom Internetu, zlonamjerni programi sve češće se stvaraju kako bi se zaradilo legalno (zlonamjerni programi se koriste za reklame) ili preko *online* prevara.

Online prevare su noviji trend Internet prevara, a obično se izvode preko *scareware* ili *ransomware* programa.

3.1. Zarazni zlonamjerni programi

Prvu skupinu zlonamjernih programa čine zarazni zlonamjerni programi. Njihova ulogu u *online* ucjenama je širenje zlonamjernih programa za ucjene na korisnička računala.

Najpoznatiji oblici zlonamjernih programa, zahvaljujući brzini širenja, su virusi i crvi. Izraz računalni virus koristi se za programe sa zlonamjernim programskim kodom koji nakon pokretanja širi virus na druga računala. Virusi mogu sadržavati i funkcije za obavljanje drugih zlonamjernih akcija. Za razliku od virusa, crv je program koji se aktivno prenosi preko mreže kako bi ugrozio druga računala. Prema tome, osnovna razlika između virusa i crva je u tome što virusi zahtijevaju korisnikovo sudjelovanje u širenju, dok se crv može proširiti automatski.

U samim počecima mreže Internet, virusi su se širili na osobna računala izmjenom programa ili sektora na disketama koji se pokreću prilikom umetanja diska (eng. boot sectors). Umetanjem kopije virusa u naredbe nekog programa ili diska, virusi bi se aktivirali svaki put prilikom pokretanja istog. Prvi računalni virusi pisani su za računalne sustave Apple II i Macintosh, ali raširili su se u vrijeme dominacije sustava IBM PC i MS-DOS. Ovakvi oblici virusa ovisili su o razmjeni programa ili disketa među korisnicima pa su se obično teže širili.

Prvi crv pojavio se 1988. godine, tzv. Internet crv ili Morris crv , a ugrozio je sustave SunOS i VAX BSD. Za razliku od virusa, nije se koristio tehnikom umetanja kopije u programe, nego je iskoristio sigurnosne ranjivosti u programima mrežnih poslužitelja te se pokretao kao odvojeni proces. Istu tehniku koriste i današnji crvi.

Širenjem platformi Microsoft Windows 90-ih godina 20. stoljeća, bilo je moguće stvarati zarazne programe u makro jezicima (pravila ili uzori koji definiraju kako se određeni ulazni niz označava na izlaznom nizu prema definiranoj proceduri). Takvi virusi ugrožavali su dokumente i predloške, a ne aplikacije.

Danas su crvi najčešće stvarani za operacijske sustave Windows, međutim postoji i mali dio crva za operacijske sustave Linux i Unix.

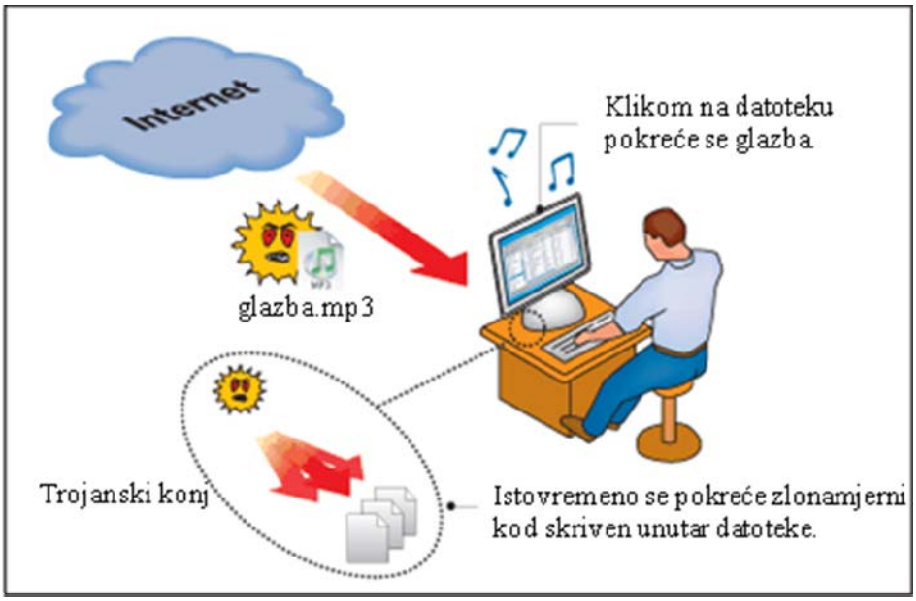
3.2. Zatajni zlonamjerni programi

U ovu skupinu zlonamjernih programa ubrajaju se trojanski konji, programi koji preuzimaju vlast nad sustavom bez znanja korisnika (eng. rootkits) te metode zaobilaženja normalne autentifikacijske procedure (eng. backdoors). Ovakvi programi također nalaze ulogu u *online* ucjenama na način da služe širenju zlonamjernih programa za obavljanje ucjena. Pri tome, razlika od zaraznih programa je način na koji se distribuiraju ti programi.

Kako bi zlonamjerni program ostvario svoj cilj, administrator sustava ne smije ga onemogućiti ili obrisati. Zatajni (eng. concealment) programi na prvom mjestu pomažu u instaliranju drugih zlonamjernih programa. Predstavljanjem zlonamjernih programa bezopasnima, korisnici dolaze u iskušenje da ih instaliraju bez znanja o tome što oni zapravo rade. Takve programi poznati su pod nazivom *trojanski konj* (eng. trojan).

Šire govoreći, trojanski konj (Slika 5) je bilo koji program koji poziva korisnike na pokretanje, a skriva zlonamjerni sadržaj koji se može aktivirati neposredno nakon preuzimanja te imati neželjene efekte na

sustav korisnika (npr. uklanjanje datoteka). Postoji oblik trojanskog konja koji se koristi za pokretanje širenja crva umetanjem istih u korisnikovu lokalnu mrežu (eng. droppers).



Slika 5 Preuzimanje i pokretanje trojanskog konja

Uporaba trojanskih konja predstavlja osnovni način distribuiranja programa za krađu korisničkih podataka (eng. spyware) na način da ih napadači ugrađuju u program koji korisnik preuzima s Interneta.

Jednom kada je zlonamjerni program instaliran na sustavu, neophodno je da ostane zatajen kako ne bi bio detektiran i uklonjen. U tu svrhu koriste se tehnike izmjene operacijskog sustava (eng. rootkits). Pomoću rootkit programa sprječava se vidljivost zlonamjernog procesa u ispisu procesa sustava ili čitanja datoteka zlonamjernog programa. Izvorno, rootkit programi su bili skupina alata koje je instalirao napadač na sustav Unix kako bi dobio administratorski (eng. root) pristup. Danas se izraz koristi općenitije za opisivanje funkcije skrivanja zlonamjernih programa. Neki zlonamjerni programi sadrže rutine za obranu od pokušaja uklanjanja na način da pokreću brojne procese koji se međusobno obnavljaju ako je to potrebno.

Metode zaobilaženja procedura autentifikacije (eng. backdoors) moguće je izvesti nakon ugrožavanja sustava, ali i prije instalacije zlonamjernih programa kako bi se napadaču omogućio pristup. Ovakve tehnike koriste napadači koji žele osigurati udaljeni pristup računalu te ostati neotkriveni, a pritom se koriste trojanskim konjima, crvima ili nekim drugim zlonamjernim programima.

3.3. Zlonamjerni programi namijenjeni zaradi

Tijekom 80-ih i 90-ih godina 20. stoljeća smatralo se da su zlonamjerni programi stvoreni kao posljedica vandalizma. Od početka 21. stoljeća veliki dio zlonamjernih programa stvara se za ostvarivanje profita napadača. Pojavljuju se mnogi programi koji su namijenjeni zaradi napadača, a oni su poslužili i kao prethodnici razvoju zlonamjernih programa za *online* ucjene. Sve češće se pojavljuju komercijalno proizvedeni programi koji imaju svrhu skupljanja informacija o korisnicima računala, prikazivanja dodatnih prozora s reklamama (eng. pop- up ads) ili upravljanja ponašanjem web preglednika (eng. spyware). Primjer su programi koji preusmjeravaju rezultate tražilice (npr. program „CoolWebSearch“) te programi koji dostavljaju oglašivačima informacije o korisnicima koji posjećuju određenu web stranicu (npr. „Zango“). Jedan od oblika ovakvog programa (eng. stealware) ima mogućnost prepisivanja kodova udruženog marketinga kako bi se prihodi preusmjerili autorima programa. Kada korisnici žele kupiti uslugu ili proizvod preko Internet mreže, zlonamjerni program instaliran u računalni sustav korisnika provjerava da se pri trgovanju koristi udruženi marketing. Ako se koristi udruženi marketing, program jednostavno zamijeni kolačiće u pregledniku s drugim kolačićima, čime preusmjerava promet na željenu stranicu. Neki poznatiji primjeri ovakvih programa su: „BUYERSPORT“, „LIMESHOP“ i SAVENOW.

Često su instalirani kao trojanski konj, a razlikuju se u tome što ih autori otvoreno predstavljaju kao poslovne programe. Također, mnogi takvi programi sadrže licencu koja predstavlja ugovor između korisnika i proizvođača. U ovom slučaju ugovor služi za zaštitu proizvođača jer korisnici većinom ne čitaju sadržaj prije prihvaćanja ugovora.

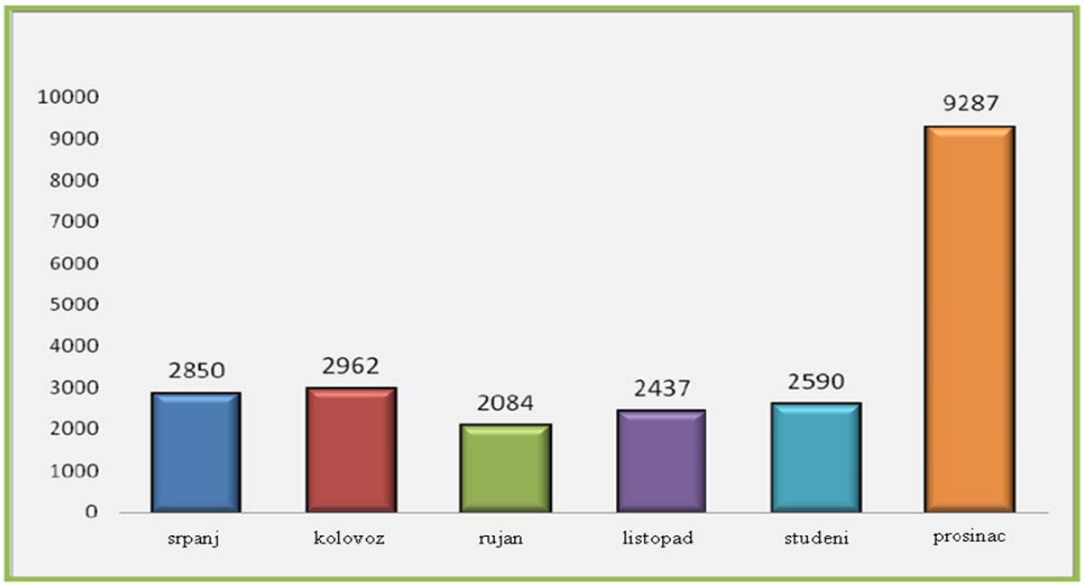
Drugi način zarade putem ugrožavanja zlonamjernim programima je korištenje ugroženih računala za obavljanje zlonamjernih aktivnosti. Često se takva ugrožena računala koriste za slanje neželjenih poruka elektroničke pošte (eng. spam) jer štite anonimnost napadača. Osim toga, napadači mogu iskoristiti računala za pokretanje DDoS (eng. distributed denial-of-service) napada. Kako bi se upravljalo aktivnošću velikog broja ugroženih računala, napadači najčešće koriste sustave poznate pod nazivom *botnet* mreža.

Osim opisanih načina zarade, autor zlonamjernog programa može krasti osjetljive podatke žrtvi. Neki zlonamjerni programi instaliraju programe (eng. key logger) koji presreću pritisnute tipke na tipkovnici prilikom upisa lozinke, broja kreditne kartice ili nekih drugih osjetljivih informacija. Prikupljene informacije automatski se prenose autoru zlonamjernog programa, omogućujući mu izvođenje bankovnih i drugih prevara. Slično tome, zlonamjerni programi mogu kopirati ključeve ili lozinke za *online* igre, što pruža mogućnost napadaču da ukrade korisničke račune i sl.

Još jedan način krađe novca preko ugroženog osobnog računala je preuzimanje kontrole nad dial-up modemom te pokretanje skupih (često međunarodnih) poziva. Postoje posebni programi (eng. dialer) koji pokreću pozive prema određenim telefonskim brojevima te ostavljaju otvorenu liniju prema brojevima sa dodatnom vrijednošću (npr. za Hrvatsku 060 brojevi).

3.4. Scareware programi

Pojam *scareware* obilježava nekoliko klasa programa za prevare, obično s ograničenim ili nikakvim profitom koji se prodaju korisnicima pod određenim neetičnim marketinškim praksama. Dizajnirani su kako bi izazvali šok ili percepciju krađe kod korisnika. Neki oblici programa koji se koriste za krađu podataka o korisnicima (eng. spyware) i programa koji automatski pokreću ili preuzimaju sadržaj s Interneta (eng. adware) koriste slične metode. Najčešće korištena taktika je uvjeravanje korisnika da im je računalo zaraženo virusom te preporučivanje preuzimanja antivirusnog programa za uklanjanje virusa. Preporučeni antivirusni programi su najčešće komercijalni pa korisnici moraju platiti njihovu uporabu Prema organizaciji *Anti-Phishing Working Group* (http://www.antiphishing.org/reports/apwg_report_H2_2008.pdf) broj takvih programa porastao je sa 2850 na 9287 u drugoj polovici 2008. godine. Podatke njihovog istraživanja prikazuje Slika 6. Također, izraz *scareware* se ponekad koristi za bilo koju aplikaciju ili virus koji se koristi za prevaru korisnika kako bi se izazvala panika.



Slika 6 Porast broja lažnih antivirusnih programa

3.4.1. Programi za prevare

Termin „programi za prevare“se često koristi za opis proizvoda koji dok obavljaju željenu radnju također proizvode puno upozorenja o potrebi za primjenom komercijalnog vatrozida (eng. firewall) ili programa za čišćenje registara tj. programa koji su dizajnirani za uklanjanje neželjenih zapisa u registrima (eng. registry cleaner software). Ovu klasu programa obilježava neprestano prikazivanje poruka upozorenja korisnicima.

Čak i neke web stranice prikazuju nove prozore s reklamama (eng. pop-up) ili reklamne poruke (eng. banners) s tekstom koji korisniku govori da mu je osobno računalo zaraženo zlonamjernim programom. Također, savjetuju skeniranje osobnog računala klikom na ponuđeni gumb kako je prikazano na slici 7.

Kako ovakvi programi ponekad nisu povezani s instaliranim zlonamjernim programima, korisnik može ugroziti računalo i pritiskom na tipku kojom otkazuje akciju ili zatvara poruku. Napadači dizajniraju poruke kako bi one izgledale kao da dolaze od operacijskog sustava.

Neki oblici programa za krađu korisničkih podataka također se kvalificiraju u *scareware* programe, jer mijenjaju pozadinu korisnikovog zaslona, instaliraju ikone (na operacijskim sustavima Windows) te neprestano obavještavaju korisnika da im je računalo zaraženo s nekim oblikom zlonamjernog programa. Ovakve postupke ne koriste legitimne anti-spyware aplikacije.

Primjer programa za prevare je „SpySheriff“. To je program za krađu podataka o korisniku (eng. spyware) koji se predstavlja kao program za uklanjanje upravo takvih zlonamjernih programa.

Slika 7 Poruka *scareware* programa

3.4.2. Program za podvale

Kao još jedan oblik *scareware* programa javljaju se programi za podvale (eng. prank software) koji su namijenjeni za zastrašivanje korisnika uporabom neočekivanih slika, zvukova ili video poruka. Prvi program ovog tipa se distribuirao za računala Amiga 1991. godine, a zvao se „NightMare“. Prilikom pokretanja, on ostaje „uspavan“ slučajno odabran period vremena te konačno mijenja cijeli izgled pozadine zaslona uz puštanje strašnog zvuka. Često se koriste programi s prikazom poruka koje stavljaju korisnika u nepovoljnu situaciju. Primjer su poruke s upitom o brisanju svih podataka s tvrdog diska te ponuđenim tipkama za prihvat, a ne odbacivanje akcije. Bez obzira na odabir mogućnosti za prihvat brisanja, podaci ostaju sačuvani. Prema tome, ovakvi programi najčešće ne uzrokuju materijalnu štetu korisnicima niti se koriste u *online* prevarama za zaradu.

3.5. Ransomware programi

Kao ozbiljniji oblik *online* prevara javljaju se programi koji „otimaju“ korisnikove datoteke te zahtijevaju novčanu „otkupninu“. Znači, radi se o zlonamjernom programu koji onemogućuju pristup operacijskom sustavu ili podacima dok korisnik ne ispati određeni novčani iznos (eng. ransom) za njegov povrat.

Obično funkcionira kao računalni crv ulazeći u sustav kroz ranjivost u mrežnim uslugama ili privitku poruke elektroničke pošte. Tada može:

- onemogućiti osnovne usluge sustava ili spriječiti prikazivanje sadržaja zaslona na početku pokretanja sustava,
- kriptirati određene osobne datoteke korisnika (ovakvi programi se nazivaju i *cryptovirus*).

U oba slučaja, zlonamjerni program može tražiti:

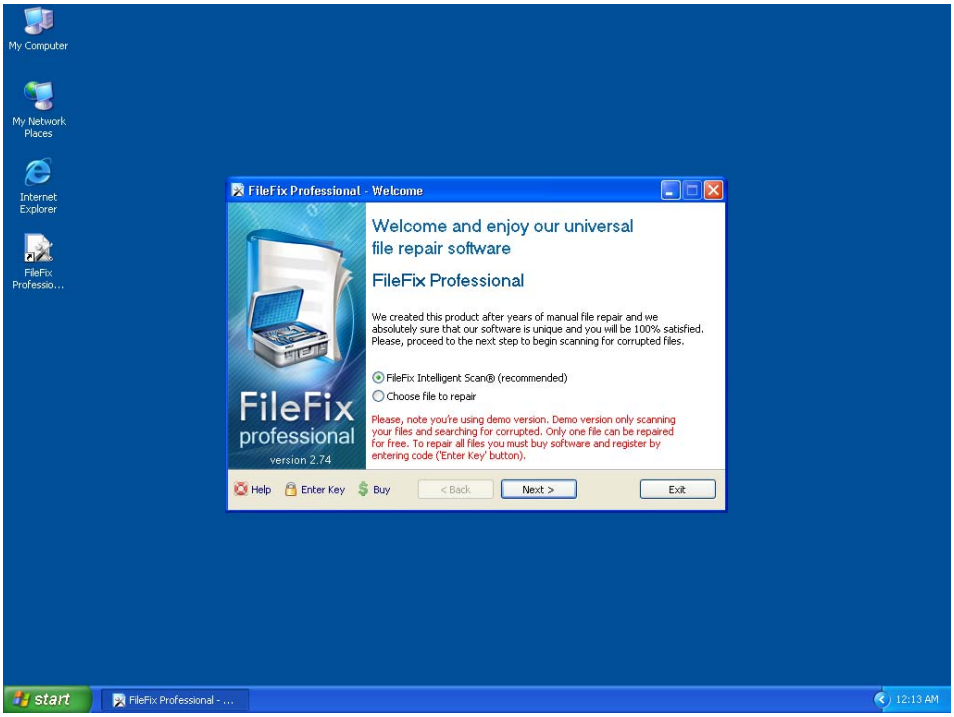
- unos koda koji je dostupan samo nakon plaćanja traženog novčanog iznosa ili slanja sms poruke,
- kupnju alata za dekriptiranje.

Sofisticiraniji programi mogu koristiti hibridno kriptiranje žrtvinih datoteka sa slučajno odabranim simetričnim ključem i fiksnim javnim ključem. Jedina strana koja zna privatni ključ potreban za dekriptiranje tada je autor zlonamjernog programa.

3.5.1. Način rada

Ransomware se definira kao program koji iskorištava ranjivost na osobnom računalu korisnika kako bi upao u sustav te kriptirao datoteke. Tada napadač zadržava datoteke zaključanim dok žrtva ne isplati određeni novčani iznos. Ako je sustav ranije bio pod napadom nekog crva ili trojanskog konja, napadač tada može jednostavnije upasti u loše konfiguriran sustav.

Prvi korak u napadu uključuje podmetanje stvorenog zlonamjernog programa korisniku ili navođenje korisnika na njegovo dobrovoljno preuzimanje (Slika 8). Obično se tada korisnici služe lažnim porukama o potrebi za preuzimanjem antivirusnih programa, umetanjem programa u razne poveznice ili privitke elektroničke pošte i sl.



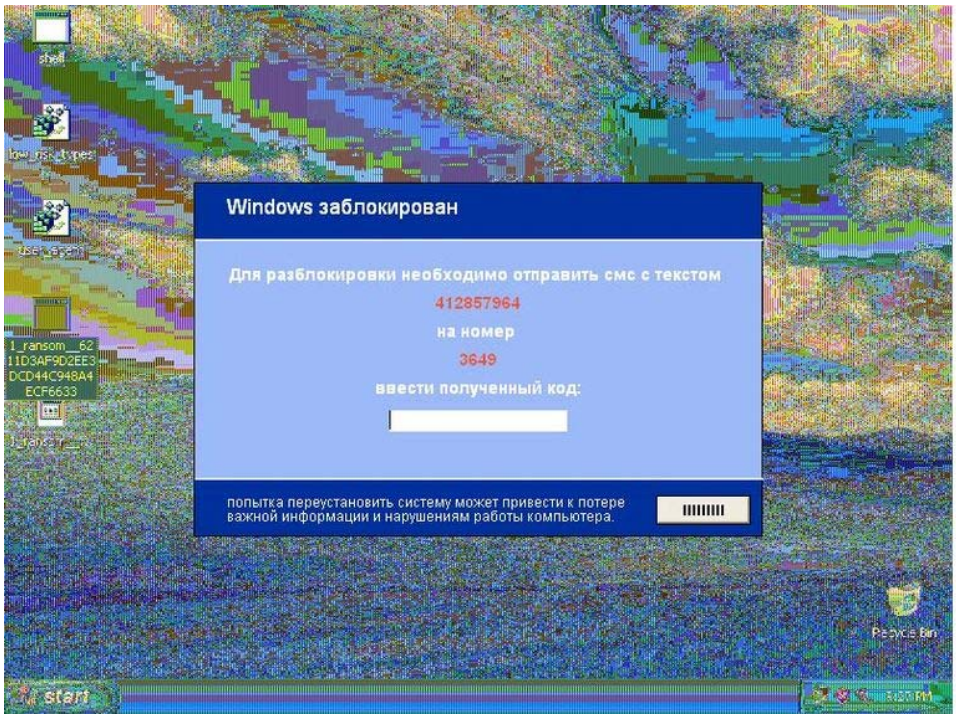
Slika 8 Navođenje korisnika na preuzimanje zlonamjernog programa

Nakon instalacije zlonamjerni program traži razne tipove važnih datoteka poput onih s nastavcima: .txt, .doc, , .ppt, .zip, .jpg, .pdf i dr. Znajući da takve datoteke sadrže korisniku bitne podatke, napadač ih kriptira čineći ih nedostupnima korisniku.

Kada napadač pronađe željene datoteke postoji nekoliko načina koje može iskoristiti za njihovo zaključavanje:

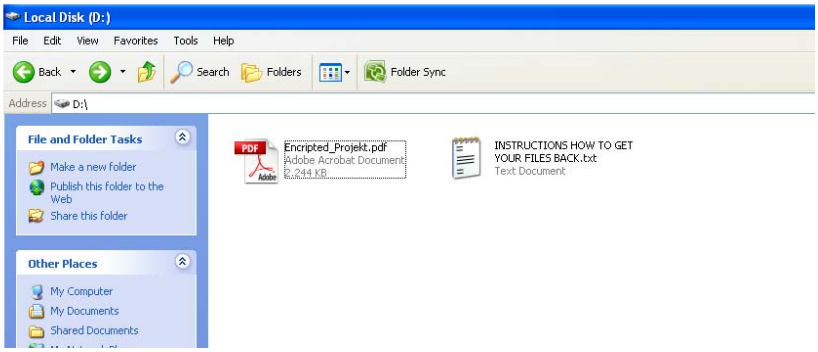
1. spremanje datoteka u lozinkom zaključanu arhivu (npr. zip arhivu) te uklanjanje originalnih datoteka sa sustava,
2. pojedinačno kriptiranje svake pronađene datoteke te uklanjanje originalnih datoteka. Na primjer, ako napadač pronađe datoteku koja se zove „Diplomski_rad.doc“, *ransomware* će stvoriti datoteku „Encripted_Diplomski_rad.doc“ kako bi označio originalnu datoteku.
3. stvaranje skrivenih direktorija te premještanje pronađenih datoteka u taj direktorij. Ova strategija nosi najmanje štete žrtvi te omogućuje korisniku s dovoljnom razinom znanja povrat datoteka bez plaćanja.

Osim kriptiranja datoteka, zlonamjerni program može imati funkciju zaključavanja korisničkog računala. Pri tome napadači se služe raznim tehnikama poput pokretanja zlonamjernog programa prilikom pokretanja računala ili sprječavanjem prikaza na zaslonu računala. Primjer ovakvog napada dan je na Slika 9.



Slika 9 Zaključavanje korisničkog računala

Sljedeći korak uključuje kontaktiranje korisnika. Napadač šalje žrtvi poruku elektroničke pošte ili se pojavljuje prozor s reklamnim oglasom (porukom) u kojoj se zahtjeva kriptirajući ključ za otključavanje datoteka. Česta praksa je i stvaranje datoteke s uputama za korisnike o mogućnosti povrata podataka (Slika 10).



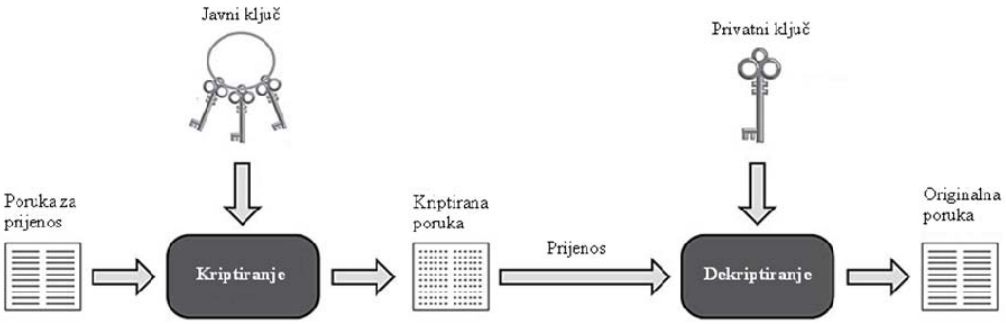
Slika 10 Upute za povratak podataka

Nadalje, kada napadači korištenjem *ransomware* alata uspješno preuzmu kontrolu nad podacima, obično ih kriptiraju sofisticiranim algoritmima. Lozinke za dekriptiranje otkrivaju se samo ako žrtva isplati traženi novčani iznos napadaču. Obično napadač obavještava žrtvu s porukom koja nosi upute o koracima za povrat podataka, a poruke se nalaze u istim direktorijima kao i kriptirani podaci.

3.5.2. Najčešće korišteni kriptografski algoritmi

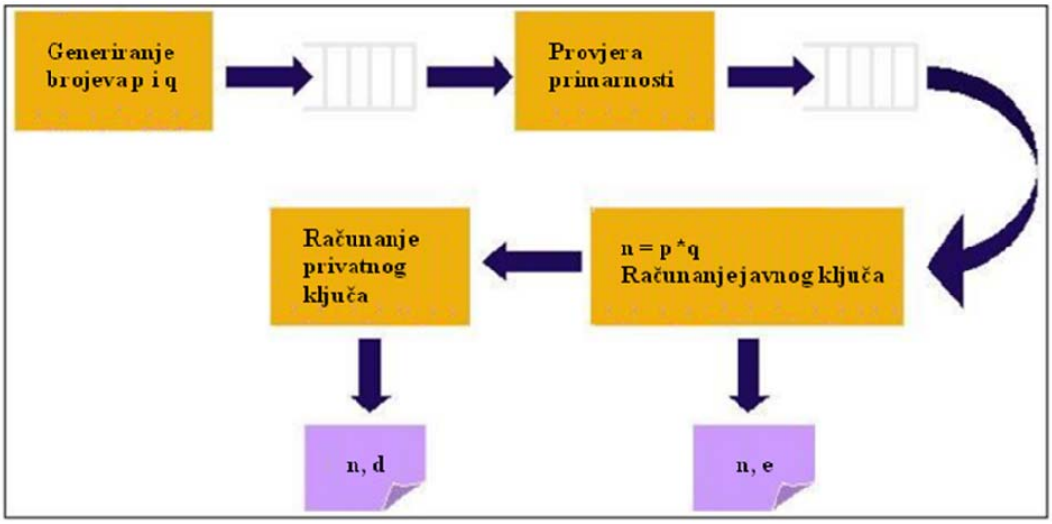
Iako su prve inačice zlonamjernih kriptirajućih programa koristile slabije algoritme, sve se češće pojavljuju programi koji koriste snažne kriptografske algoritme. Jedan od najčešće korištenih je algoritam RSA (za kriptografiju uporabom javnog ključa). Spomenuti algoritam se koristi za izmjenu ključeva kod TLS (eng. Transport Layer Security) i SSL (eng. Secure Socket Layer) protokola.

Algoritam RSA uvodi uporabu javnog i privatnog ključa. Javni ključ je poznat svim korisnicima te se koristi za kriptiranje poruke. Poruka koja je kriptirana javnim ključem može se dekriptirati samo pomoću privatnog ključa. Znači, korisnik A kriptira poruku javnim ključem korisnika B te mu ju prosljeđuje. Korisnik B uporabom privatnog ključa dekriptira poruku. Opisani scenarij prikazan je na **Error! Reference source not found.**.



Slika 11 RSA algoritam

Navedeni ključevi generiraju se preko složenih matematičkih izraza uporabom slučajno generiranih primarnih brojeva. Zatim se računaju parametri javnog i privatnog ključa kako je prikazano na slici 12. Javni se ključ sastoji od modula n i eksponenta e, a privatni od modula n i eksponenta d. Sigurnost algoritma proizlazi iz složenosti faktorizacije velikih brojeva.



Slika 12 Računanje privatnog i javnog ključa

3.5.3. Nemogućnost otkrivanja napadača

Autori zlonamjernih programa za *online* ucjene u većini slučajeva ostaju neotkriveni i nekažnjeni. Razlog tomu je uporaba tvrtki koje su većinom registrirane u Rusiji i komuniciranje preko kineskih IP adresa. Također, napadači obično otvaraju bankovne račune na koje žrtve mogu uplaćivati novac. Takvi računi su obično samo virtualni, što znači da se novac brzo prebacuje na druge račune.

Kao primjer dan je jedan od novijih zlonamjernih programa „PGPCoder" koji se pojavio 2008. godine, a koristi RSA 1024 kriptiranje. Za sada je poznato da napadači koriste dvije ruske tvrtke kako bi ucjenjivali korisnike.

Jedan od ucjenjivača, poznat pod nazivom *John Dow-ish* kontaktira žrtve sa IP adrese 58.38.8.211 (registrirana na: Liaoning Province Network China Network Communications Group Corporation No.156,Fu-Xing-Men-Nei Street, Beijing 100031). Zahtijeva uplatu od $100 na račun Liberty Reserve U6890784 ili E-Gold 5431725.

Drugi napadač, Paul Dyke, koristi IP adresu 221.201.2.227 (Liaoning Province Network China Network Communications Group Corporation No.156,Fu-Xing-Men-Nei Street, Beijing 100031). Za dekriptiranje datoteka traži iznos od $200, koji je potrebno uplatiti na račun E-Gold 5437838 ili Liberty Reserve U6890784.

Adrese elektroničke pošte kojima se koriste autori programa su:

- content715@yahoo .com,
- saveinfo89@yahoo .com,
- cipher4000@yahoo .com ili
- decrypt482@yahoo .com.

Iako postoje sigurnosne organizacije (poput FireEye, Kaspersky Lab., Dr.Web i sl.) koje prate zlonamjerne radnje, u većini slučajeva korisnici nisu spremni na suradnju. Većina onih koji su pogođeni nekom *online* ucjenom plaćaju napadaču traženi novčani iznos kako bi dobili svoje podatke. Bolja praksa u ovom slučaju bilo bi kontaktiranje sigurnosnih organizacija, a većina od njih savjetuje korisnicima odbijanje ponude napadača za kupnjom nekog proizvoda ili zahtjeva za isplatom nekih novčanih iznosa. Takve organizacije često nude korisnicima programe za dekriptiranje koji mogu besplatno obnoviti zaključane datoteke.

4. Primjeri online ucjena

4.1. Scareware programi

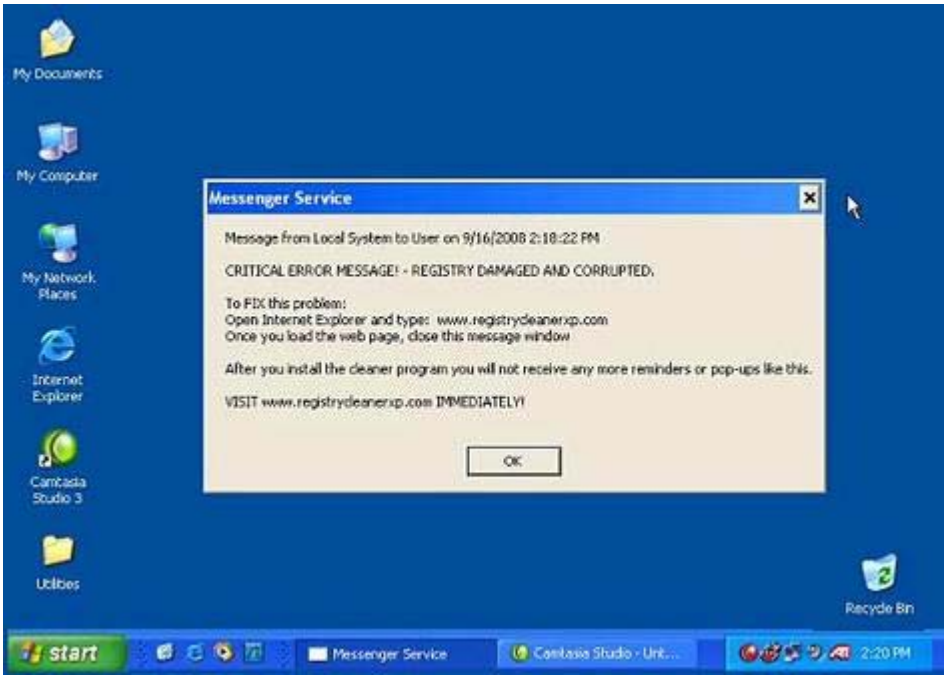
Postoji više primjera izrade *scareware* programa za operacijske sustave Windows:

- Godine 2005. Tvrtka Microsoft i država Washington optužili su tvrtku Secure Computer koja je izradila program „Spyware Cleaner" za uporabu poruka o *scareware* programu. Navedeni tvorci zlonamjernog programa morali su platiti odštetu od milijun dolara. Zlonamjerni program koristio je prozore koji se pokreću s pregledom web stranica kao tehniku navođenja korisnika na preuzimanje lažnog *antispyware* programa. Osim toga, program je brisao datoteku „Hosts" koja se koristila za blokiranje neželjenih web stranica. Nešto više informacija moguće je pronaći na web stranici:

  http://blogs.zdnet.com/Spyware/?p=759

- U listopadu 2008. godine tvrtka Microsoft podigla je tužbu protiv dvije tvrtke u Texasu: Branch Software i Alpha Red zbog stvaranja zlonamjernog programa „Registry Cleaner XP". Tvrtke su koristile prozore s reklamama koje se pokreću prilikom posjećivanja web stranica, prikazane na slici 9, s upozorenjem o oštećenju registara te uputama o posjeti web stranice i preuzimanju spomenutog programa uz naplatu od 39,95 USD. Više detalja o spomenutom slučaju moguće je pročitati na sljedećoj poveznici:

  http://news.cnet.com/8301-1009_3-10053565-83.html



Slika 13 Lažna poruka o oštećenju registra

Osim tvrtke Microsoft, sličnu tužbu podigla je tvrtka Federal Trade Commicion u prosincu 2008. godine protiv dvije tvrtke u SAD-u. Radi se o tvrtkama Innovative Marketing, Inc. i ByteHosting Internet Services koje su odgovorne za reklamiranje aplikacija WinFixer, WinAntivirus, DriveCleaner, ErrorSafe i XP Antivirus. Utvrđeno je da su uspjeli prevariti više od milijun korisnika u SAD-u da kupe njihove lažne proizvode.

Popis brojnih lažnih i sumnjivih programa, kao i web stranica koje ih sadrže moguće je pogledati preko poveznice:

http://www.spywarewarrior.com/rogue_anti-spyware.htm

Jedan od aktualnih primjera ovakvih prevara javlja se među rezultatima pretrage o padu aviona Air France Flight 447. Pretragom za novostima o avionskoj nesreći dobiju se poveznice čijim se posjećivanjem pokreće preusmjeravanje na razne stranice, što konačno vodi do preuzimanja lažnog antivirusnog programa „Install_2022.exe". Putanju preusmjeravanja prikazuje slika 10 Prikazane URL adrese detektirane su kao:

- hxxp:// cnnnews2009.{BLOCKED}.com/french-airbus-crash.html – HTML_REDIRECT.ED.
- hxxp:// cnnnews2009.{BLOCKED}.com/images/menu.js – JS_CRYPTED.HW.
- hxxp://{BLOCKED}ware-live-scanv3.com/1/?id=2022&smersh=8186a276d&back=%3DDQwxDDwNcQNMI%3DN/My computer Online Scan.htm – JS_FAKEAV.BIM.

Slika 14 Preusmjeravanje do lažnog antivirusnog programa

Lažni antivirusni program „Install_2022.exe" je zapravo trojanski konj „Troj_FakeAv.bim" koji se nakon pokretanja spaja na URL adresu za preuzimanje drugog trojanskog konja zvanog „Troj_Yekatel.aa". Prilikom pokretanja, drugi trojanski konj prikazuje preporuku za instaliranje aplikacije zvane „Personal Antivirus". Ako se prihvati instalacija, pojavljuje se poruka o detekciji brojnih zlonamjernih programa na sustavu. Riječ je o lažnoj poruci koja se koristi kako bi se prestrašili korisnici te naveli na preuzimanje potpune inačice antivirusnog programa. Detaljniji opis ovog problema moguće je pročitati na stranicama:

http://blog.trendmicro.com/search-results-for-air-france-flight-447-lead-to-rogue-antivirus/

4.2. Ransomware programi

Prvi poznati ransomware program pojavio se 1989. godine pod nazivom „PC Cyborg Trojan“, a kriptirao je imena datoteka slabim kriptografskim šiframa. Praksu uporabe kriptografije s javnim ključem za ovakvu vrstu napada uveo je Young 1996. godine predstavljajući zlonamjerni program za platformu Macintosh SE/30.

Primjeri sličnih zlonamjernih programa pojavili su se u svibnju 2005. godine. Do sredine 2006. godine crvi poput Gpcode, TROJ:RANSOM.A, Archiveus, Krotten, Cryzip i May Archive počeli su koristiti sofisticirane kriptografske algoritme (RSA).

http://www.theregister.co.uk/2006/07/24/ransomware/

Godine 2007. sigurnosne organizacije PandaLabs i Kaspersky Lab identificirale su trojanskog konja koji kriptira korisničke podatke te ostavlja obavijest o potrebi za isplatom 300 dolara za ključ. Autor zlonamjernog programa u poruci je istaknuo kako je koristio algoritam RSA-4096 te dao upute korisnicima o mogućnosti povratka datoteka (Slika 15).

Hello, your files are encrypted with RSA-4096 algorithm (http://en.wikipedia.org /wiki/RSA).

You will need at least few years to decrypt these files without our software. All your private information for last 3 months were collected and sent to us.

To decrypt your files you need to buy our software. The price is $300.

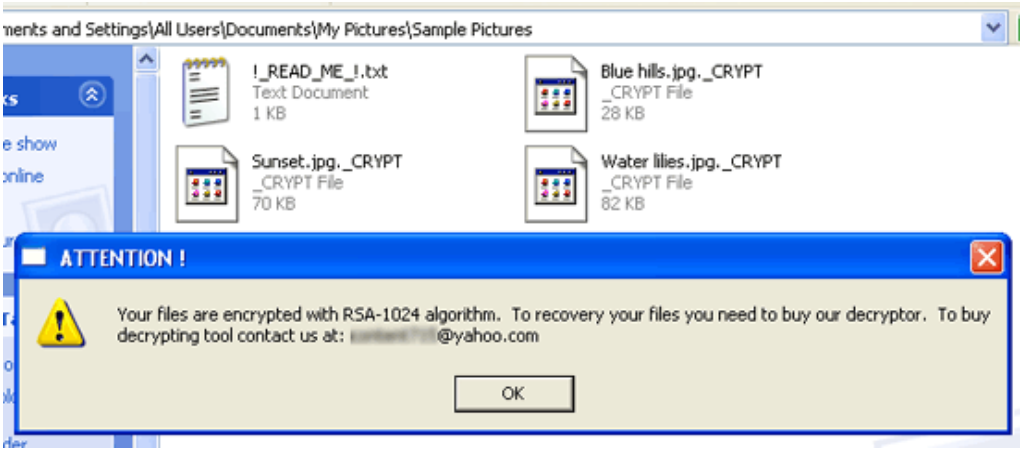
To buy our software please contact us at [e-mail address varies] and provide us with your personal code [code varies]. After successful purchase we will send your decrypting tool, and your private information will be deleted from our system.

If you will not contact us until 07/15/2007 your private information will be shared and you will lost all your data.

Glamorous team

Slika 15 Poruka zlonamjernog programa

U lipnju 2009. godine otkriven je program „Gpcode.AK“ koji koristi kriptografski algoritam RSA s ključevima duljine 1024 bita. Spomenuti zlonamjerni program kriptira datoteke različitih formata uključujući .doc, .txt, .pdf, .xls, .jpg, .png, .cpp i .h. Autor programa „GPcode“ je proveo dvije godine poboljšavajući virus, ispravljajući pogreške te uvođenje ključa od 1024 bita. Nakon što program kriptira datoteke na žrtvinom računalu dodaje nastavak ._CRYPT te stvara datoteku naziva !_READ ME_!..txt u istom direktoriju. Pomoću te datoteke korisnici se obavještavaju o kriptiranju datoteka i potrebi za kupnjom programa za dekriptiranje.

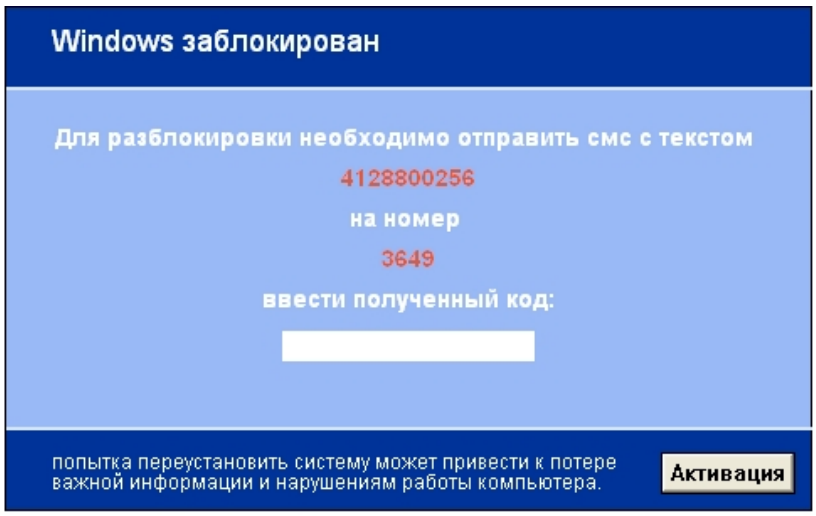


Slika 16 Kriptirane datoteke pomoću trojanskog konja „GPcode.AK“

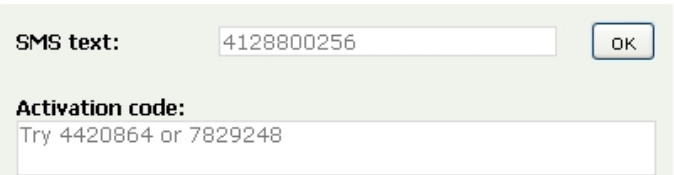
Više informacija o opisanom programu moguće je pronaći na stranici:

http://www.kaspersky.com/news?id=207575650

2009. godine otkriveni su ransomware programi koji zaključavaju ugroženo korisničko računalo te zahtijevaju unos koda za njegovo otključavanje. Program je nazvan „Trj/SMSlock.A“, a nakon zaključavanja računala upućivao je korisnika na slanje SMS poruke s jedinstvenim brojem na ponuđeni broj kako bi se primio deaktivacijski kod. Rad programa sličan je ranije otkrivenim programima nazvanim „Trojan-SMS.Python.Flocker“ i „RedBrowser“. Postoje različite sigurnosne organizacije koje se bore protiv ovakvih online prevara, a jedna od njih je i Dr.Web, koja je objavila besplatni generator deaktivacijskih kodova (Slika 17) kako korisnici ne bi morali plaćati autoru.



Trojan.Winlock can remove itself in two hours after launching. Users who don't want to wait that long can use the web-form to enter the text of the suggested SMS and get the unblock code.



Slika 17 Generator deaktivacijskih kodova

5. Zaštita od napada

5.1. Vatrozid

Jedan od osnovnih alata za zaštitu računalnog sustava ili mreže koji je dizajniran za blokiranje neovlaštenog pristupa ja vatrozid (eng. firewall). Riječ je o uređaju ili skupu uređaja konfiguriranih kako bi spriječili ili proslijedili promet između sigurnosnih domena pomoću skupa pravila i kriterija. Moguće ih je implementirati u sklopovlju ili kao program te kao kombinaciju te dvije metode.

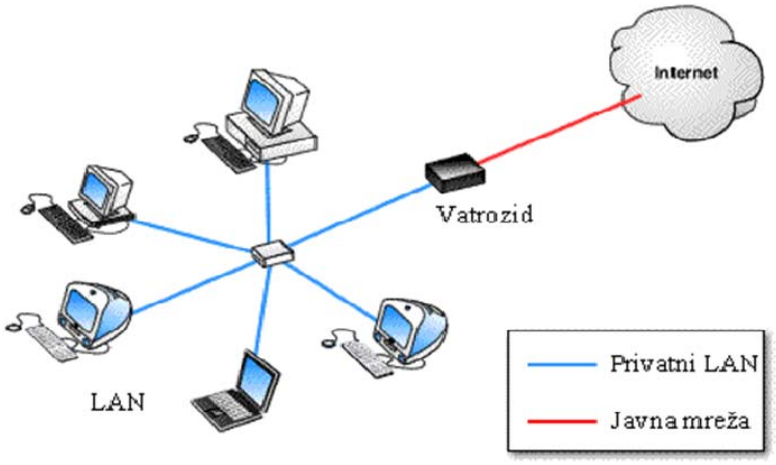
Budući da scareware i ransomware obično uključuju raznolike zlonamjerne programe, ugradnjom vatrozida moguće je spriječiti širenje tih programa na osobno računalo. Najčešće se koriste kako bi se spriječio pristup neovlaštenih korisnika privatnim mrežama koje su spojene na Internet (Slika 18). Sve dolazne i odlazne poruke prolaze kroz vatrozid koji provjerava svaku od njih te blokira one koje ne zadovoljavaju definirane sigurnosne kriterije. Prema tome, korisnici mogu ograničiti pregled određenih web stranica, preuzimanje datoteka i sl., što otežava napadačima distribuciju zlonamjernih programa.

Postoji nekoliko tipova tehnika korištenih u vatrozidu, a u nastavku su opisane neke koje se mogu iskoristiti kao zaštita od online ucjena:

Filtar paketa – provjeravanje svakog ulaznog i izlaznog paketa te njegovo prihvaćanje ili odbacivanje. Odluka o prihvaćanju i odbacivanju paketa donosi se preko skupa pravila koje definira korisnik. Ova tehnologija je vrlo efektivna i transparentna korisnicima, ali nije jednostavna za konfiguriranje. Osim toga, ranjiva je na postupke stvaranja IP (eng. Internet Protocol) paketa s lažnom izvorišnom adresom sa svrhom skrivanja identiteta pošiljatelja ili lažnog predstavljanja (eng. IP spoofing). Ipak, opisana tehnika je jedna od osnovnih metoda zaštite od neželjenog prometa na Internetu pa se preporuča korisnicima kao jedna od mogućih zaštita od preuzimanja zlonamjernih programa.

C-L (eng. Circuit-level) poveznik – prilagodba sigurnosnih mehanizama u slučajevima kada je uspostavljena TCP (eng. Transmission Control Protocol) ili UDP (eng. User Datagram Protocol) veza. Jednom kada se uspostavi veza, paketi se mogu prosljeđivati bez daljnjih provjera. Tehnika je vrlo učinkovita u zaštiti od podmetanja zlonamjernih programa korisnicima jer se stvara sigurna veza.

Posrednički poslužitelj – presretanje svih ulaznih i izlaznih poruka u mreži. Ugradnjom ovakvog poslužitelja u mreži, omogućuje se praćenje svog prometa te izoliranje zlonamjernih paketa prije širenja po cijeloj mreži.



Slika 18 Vatrozid

5.2. Blokiranje pop-up prozora

Osnovni način propagiranja scareware programa je uporaba prozora s reklamama i oglasima (eng. pop-ups). Pokreću se prilikom pregleda nekih web stranica, na način da se u novom prozoru prikazuje reklama ili oglas. Najčešće se generiraju korištenjem JavaScript koda.. Jedan od oblika ovakvog oglašavanja je uporaba prozora koji se skrivaju ispod aktivnog prozora (eng. pop-under). Riječ je o prozorima s reklamama koji se pojavljuju prilikom pregleda neke web stranice u pozadini za razliku od pop-up dodataka. Budući da ne prekidaju korisnika u istom trenutku kad se pojave, dosta je teško otkriti koje ih web stranice sadrže. Primjer pokretanja skrivenog prozora (http://www.yahoo.com/) je moguće pogledati posjetom web stranice:

http://www.javascriptkit.com/script/script2/popunder.shtml

Prvi web preglednik koji je uključio alate za blokiranje opisnih prozora bio je Opera, a slijedio ga je preglednik Mozilla Firefox uvodeći blokiranje iskakanja prozora koji se generiraju prilikom učitavanja stranice. Na početku 2000. godine, svi poznatiji web preglednici, osim preglednika Internet Explorer, omogućili su skoro u potpunosti korisnicima blokiranje neželjenih prozora s reklamama. 2004. godine tvrtka Microsoft izdala je paket nadogradnje za operacijski sustav Windows XP – Service Pack 2 koji je dodao blokiranje ovakvih prozora kod preglednika Internet Explorer.

Mnogi moderni web preglednici dolaze s ugrađenim alatima za blokiranje opisanih pop-up prozora. Takvi alati imaju više mogućih načina rada:

blokiranje svih/nijednog prozora,

blokiranje neželjenih prozora,

sastavljanje popisa prihvatljivih prozora,

blokiranje prozora s određenih web stranica,

ponovno otvaranje zatvorenih prozora.

Popis alata i programa za blokiranje takvih prozora moguće je pronaći preko poveznice:

http://en.wikipedia.org/wiki/List_of_pop-up_blocking_software

Blokiranjem poruka preko kojih se propagiraju vrste zlonamjernih programa za online ucjene moguće se zaštiti od pokretanja sličnog programa.

5.3. Antivirusni programi i IDS

Antivirusni programi su namijenjeni sprječavanju ili uklanjanju računalnih virusa, crva i trojanskih konja. Neke inačice ovih programa mogu detektirati i ukloniti programe koji automatski prikazuju ili preuzimaju određeni sadržaj s Interneta (eng. adware), programe koji služe za prikupljanje podataka o korisniku (eng. spyware) i druge oblike zlonamjernih programa. Navedene funkcionalnosti glavni su razlog zbog kojeg se preporuča njihovo stalna uporaba kao jedan od oblika zaštite sustava od programa za online ucjene. Pri tome, potrebno je koristiti najnovije inačice takvih sustava te omogućiti njihovo automatsko ažuriranje.

Postoji nekoliko metoda koje antivirusni programi koriste za otkrivanje zlonamjernih programa:

- Detekcija temeljena na potpisima – najčešće korištena metoda koja za identificiranje zlonamjernih programa uspoređuje sadržaj datoteke s rječnikom potpisa virusa. Ovakva tehnika može se koristiti kada su zlonamjerni programi otkriveni, ali ne i neposredno nakon njihova stvaranja. Prema tome, alati koje rade na ovo principu dobra su zaštita od napada zlonamjernih programa za *online* ucjene tek nakon što ih neka sigurnosna organizacija detektira.
- Detekcija zlonamjernih aktivnosti – antivirusni programi pregledaju sustav tražeći zlonamjerne aktivnosti, tj. sumnjive programe. Ovakve se tehnike mogu koristiti i za otkrivanje nepoznatih virusa. Uporaba ovakvog tipa programa omogućuje pouzdaniju zaštitu od *online* napada jer se

detekcija omogućuje u trenutku kada se primijeti zlonamjerna radnja, a ne kada program postane javno poznat.

- Heuristička detekcija – ove tehnike omogućavaju detekciju još nepoznatih zlonamjernih programa. Predstavljaju najpouzdaniju metodu zaštite od programa stvorenih za *online* ucjene jer koristi sofisticirane tehnike pregleda sustava. Dvije su osnovne metode:
    - Analiza datoteka – pretraga sumnjivih datoteka kako bi se pronašao zlonamjerni programski kod. Nedostatak ovakvih postupaka je velika količina podataka koje treba analizirati svakodnevno što uzrokuje sporost operacija.
    - Simulacija datoteka – pokretanje programa u virtualnom okruženju te zapisivanje akcija koje program izvodi. Preko zapisa antivirusni program određuje da li se radi o zlonamjernom programu.

Popis antivirusnih programa nalazi se na sljedećoj poveznici:

http://en.wikipedia.org/wiki/List_of_antivirus_software

IDS (eng. Intrusion detection system) sustavi su programi koji su dizajnirani kako bi detektirali neželjene pokušaje pristupa, manipuliranja ili onemogućavanja računalnog sustava većinom preko Interneta. Mogu se koristiti kao zaštita od programa za online ucjene jer omogućuju detekciju nekoliko tipova zlonamjernog ponašanja:

- napade na ranjive usluge,
- napade na aplikacije,
- napade povećanja povlasti,
- neovlašteni pristup,
- pristup osjetljivim podacima ili
- pojavu zlonamjernih programa.

Prilikom ugradnje IDS sustava korisnik može odabrati jedan od sljedećih tipova:

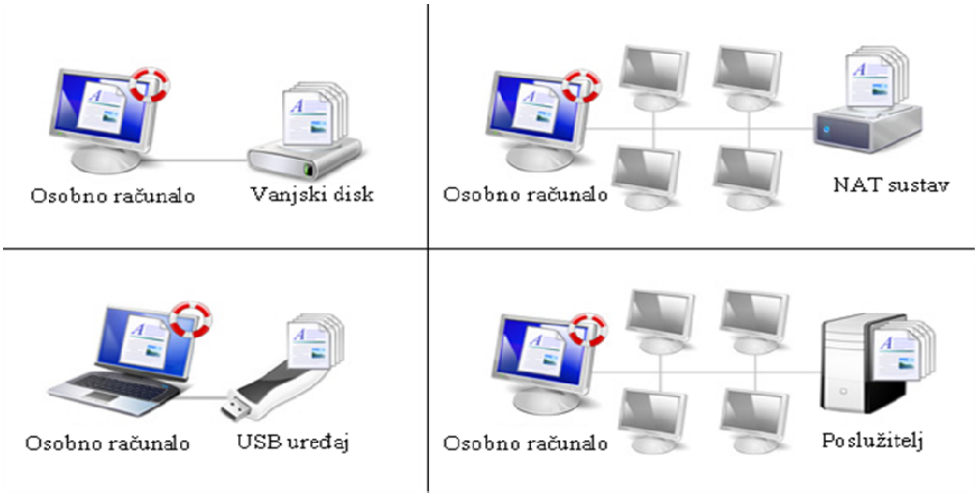
- NIDS (eng. network intrusion detection system) je neovisna platforma koja identificira upade provjerom mrežnog prometa i upravljanjem čvorovima. Između ostalog omogućuju detekciju pokušaja upada u računalne sustave. Često se koriste u kombinaciji s drugim sustavima za zaštitu pa se mogu koristiti za osvježavanje popisa neželjenih IP adresa. Ovim se postupkom sprječava posjećivanje web stranica na kojim se primjećuju zlonamjerni programi koji mogu biti stvoreni i za online ucjene.
- HIDS (eng. host-based intrusion detection system) je agent na čvoru koji identificira upad analiziranjem sustavnih poziva, zapisa aplikacije, izmjena datotečnog sustava i sl. Budući da imaju mogućnost detekcije bilo kakve izmjene na sustavu, vrlo su pouzdani kao moguća zaštita od napada zlonamjernih programa za online ucjene jer i njihova instalacija na sustavu ostavlja određeni trag.
- Hibridni IDS je kombinacija prethodno opisanih tehnika.

5.4. Obnavljanje inačica operacijskog sustava i preglednika

Proizvođači računalnih programa svakodnevno objavljuju programska rješenja za razne sigurnosne ranjivosti otkrivene u radu njihovih proizvoda. Ovo uključuje ispravke pogrešaka, izmjenu grafike te poboljšanje funkcionalnosti.

Zlonamjerni programi za online prevare najčešće upadaju u računalne sustave iskorištavajući ranjivosti u operacijskim sustavima ili preglednicima. Zbog toga je neophodno svakodnevno osvježavati inačice korištenih programa, kao i operacijskog sustava. Time se sprječava napadače da zlouporabljuju već poznate ranjivosti. Sigurnosne kopije podataka

Najjednostavniji način rješavanja problema koji donose ransomware programi je obnavljanje kriptiranih ili zaključanih podataka sa sigurnosnih kopija. Prilikom izrade sigurnosnih kopija važni se podaci pohranjuju odvojeno od izvornih datoteka, obično na vanjske diskove. Slika 19 prikazuje načine pohrane sigurnosnih kopija. Prema tome, kada zlonamjerni program kriptira podatke na računalu, korisnik još uvijek ima kopije istih na udaljenom mjestu. Ovakvim postupkom spriječen je gubitak podataka, ali i potreba za plaćanjem traženih novčanih iznosa napadačima kako bi se dobio ključ za dekriptiranje datoteka. Ipak, potrebno je imati na umu da nije dovoljno obnoviti podatke sa sigurnosnih kopija jer je zlonamjerni program i dalje prisutan na računalu. Prije postupka obnavljanja podataka korisnik treba osvježiti inačicu operacijskog sustava i ukloniti zlonamjerni program, ispravno konfigurirati vatrozid te instalirati trenutne inačice antivirusnog programa.



Slika 19 Izrada sigurnosnih kopija

Postoje razni alati koji obavljaju izradu sigurnosnih kopija, a neki osnovni navedeni su na sljedećoj poveznici:

http://en.wikipedia.org/wiki/List_of_backup_software

Osim pohrane kopije podataka na vanjski disk, korisnik može stvoriti sliku diska. Slika diska je datoteka ili uređaj za pohranu koji sadrži potpuni sadržaj i strukturu uređaja za pohranu (npr. tvrdog diska). Obično se stvara kopiranjem sektor po sektor izvornog medija.

Popis alata koji obavljaju ovakve postupke nalazi se na web stranici:

http://en.wikipedia.org/wiki/List_of_disk_imaging_software

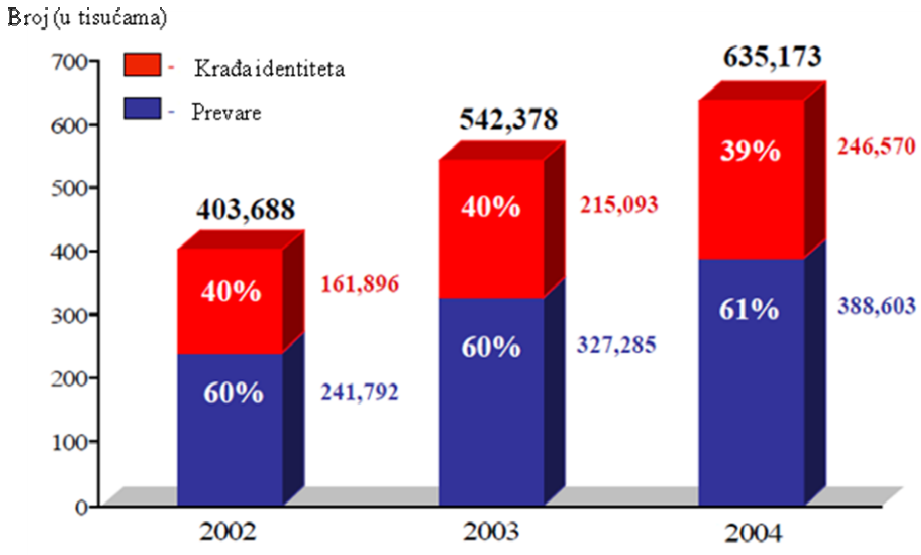
5.5. Ostali savjeti za zaštitu

Čak i uz uporabu raznih sustava za zaštitu, stvaranja sigurnosnih kopija i obnavljana inačica korištenih programa, korisnici se trebaju pridržavati nekih dodatnih mjera kako bi izbjegli online ucjene. U nastavku je nekoliko osnovnih savjeta za svakog korisnika Interneta:

- Prilikom pregleda Internet stranica potrebno je dobro razmisliti o posjećivanju poveznica postavljenih na web stranicu. Vrlo često poveznice ne vode do sadržaja na koji ukazuje tekst. Osim toga, napadači često uvode tehnike kojima korisnika preusmjeravaju do automatskog preuzimanja zlonamjernih programa.
- Osim poveznica, potrebno je izbjegavati posjećivanje reklamnih dodataka i poruka o osvajanju nagrada, pokretanje video zapisa ili prihvaćanje ponuda za *online* skeniranjem osobnog računala. Takvim se trikovima napadači najčešće koriste kako bi naveli korisnika na preuzimanje njihovih zlonamjernih programa.
- Kao jedan od mogućih načina izbjegavanja prozora s reklamnim porukama je onemogućavanje pokretanja Java ili JavaScript koda u web pregledniku. Postupak je vrlo funkcionalan jer je većina takvih poruka stvorena upravo preko navedenih tehnika.
- Korisnicima se također savjetuje odbacivanje sve neželjene elektroničke pošte poput oglasa, reklama i ponuda raznih proizvoda ili usluga. Posebno je važno pripaziti na privitke u porukama elektroničke pošte jer je to jedan od osnovnih načina distribucije programa za *online* ucjene. Zbog toga korisnicima se savjetuje odbacivanje privitaka koji su došli s nepoznatih izvora, ali i onih koji su sumnjivi ili neočekivani, a dolaze s poznatih izvora. Jedan od načina na koji je moguće detektirati zlonamjerni kod u pritku poruke elektroničke pošte je omogućavanje skeniranja svih poruka nekim antivirusnim programom.
- Dodatnu zaštitu moguće je postići određenim postavkama i načinom rukovanja računalom. Korisnici bi trebali onemogućiti skrivanje nastavaka imena datoteka, kao i isključiti mogućnost dijeljenja datoteka. Također, u slučaju detekcije nepoznatog programa na sustavu, takav se program ne bi trebalo pokretati.

6. Očekivanja u budućnosti

Prema izvješću „National and State Trends in Fraud & Identity Theft“ (http://www.consumer.gov/sentinel /pubs/Top10Fraud2004.pdf) količina Internet prevara raste iz godine u godinu. Statistički podaci dani su na Slika 20, a prikazuju porast od 146 811 *online* prevara u razdoblju od 2002. do 2004. godine.



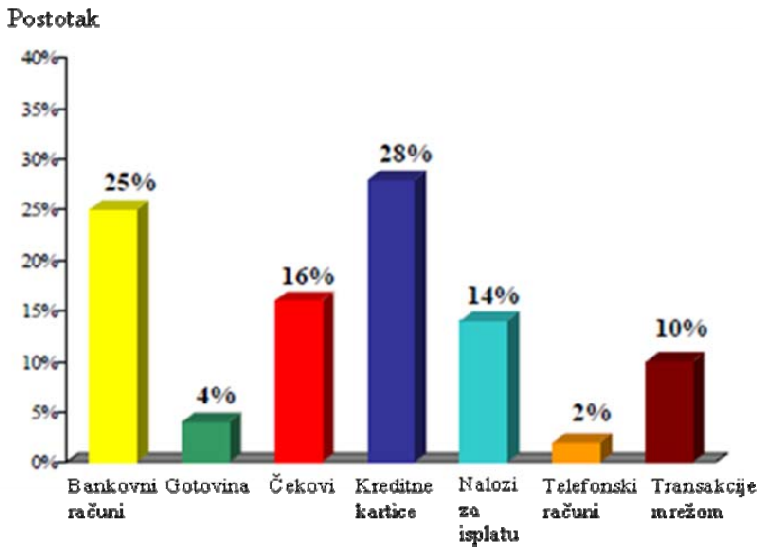
Slika 20 Statistički podaci o Internet prevarama

Isto istraživanje navodi da su ukupni troškovi uzrokovani *online* ucjenama 2004. godine bili veći od pola milijarde USD (točna procjena iznosi $547,854,781). Također, 30 % korisnika koji su žrtve *online* ucjena ne plaćaju tražene iznose, dok 4 % njih isplaćuju i više od $5 000 (Slika 21).

Isplaćeni iznos	Postotak
$0	30%
$1 - 25	7%
$26 - 50	7%
$51 - 75	4%
$76 - 100	4%
$101 - 250	12%
$251 - 500	11%
$501 - 1,000	8%
$1,001 - 5,000	12%
Više od $5,000	4%

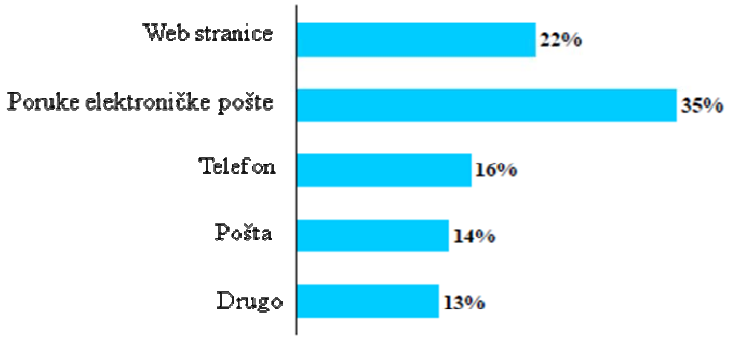
Slika 21 Postotak isplaćenih novčanih iznosa

Napadači se koriste raznim tehnikama naplate traženih novčanih iznosa, a najčešći način je preko kreditnih kartica (28 %) i bankovnih računa (25 %). Ostali podaci prikazani su na Slika 22.



Slika 22 Najčešći načini isplate novčanih iznosa

Najčešće tehnike kontaktiranja korisnika uključuju kreiranje web stranica ili slanje poruka elektroničke pošte. Ipak, nije isključeno i reklamiranje putem telefona ili pošte, a ukupna statistika prikazana je na Slika 23.



Slika 23 Tehnike kontaktiranja korisnika

Uzimajući u obzir iznesenu statistiku o količini i troškovima online ucjena, , može se očekivati povećanje broja zlonamjernih programa za izvođenje ucjena. Ovakva pretpostavka posljedica je njihove jednostavne propagacije putem poruka u prozorima sa reklamama koje se pojavljuju prilikom pregleda nekih web stranica. Napadači smišljaju različite metode i tehnike za navođenje korisnika na preuzimanje lažnih programa. U budućnosti se može očekivati veća pojava lažnih poruka koje se pokreću prilikom prikaza web stranice, ali i tijekom posjećivanja poveznica ili pregleda sadržaja iste web stranice. Napadači će sve češće koristiti popularne web stranice, kao i poznate osobe i važne događaje za privlačenje korisnika na uporabu programa.

Što se tiče *ransomware*-a, također se očekuje povećanje broja takvih zlonamjernih programa za *online* ucjene. Osim toga, predviđa se povećana uporaba modernijih kriptografskih tehnika ili postupaka zaključavanja datoteka. Budući da su te sofisticirane tehnike obično složene, neće ih biti moguće ukloniti bez kontaktiranja napadača i kupnje odgovarajućeg ključa. Prve inačice programa koristile su ključeve duljine 50 bita što osobama sa dovoljnim informatičkim znanjem nije predstavljalo problem u dekriptiranju. Ipak, daljnji razvoj ovakvih zlonamjernih programa doveo je do uporabe ključeva duljine 260 bita, zatim 330 bita te 660 bita. Dekriptiranje podatka kriptiranih ključem duljine 660 bita uz uporabu računala od 2,2 GHz trajalo bi oko 30 godina. Međutim, pojavile su se inačice programa koje koriste algoritam RSA s duljinom ključa od 1024 bita, a moguće je očekivati i daljnja poboljšanja (povećanje duljine ključa, noviji algoritmi). Dekriptiranje podataka kriptiranih ključem duljine 1024 bita na jednom računalu trajalo bi milijune godina, a tek kad bi se moglo uključiti 15 milijuna modernih računala ovo bi se vrijeme smanjilo na samo godinu dana. Korisnici bi mogli

doći u situaciju u kojoj nemaju drugog izlaza osim plaćanja traženog novčanog iznosa kako bi dobili svoje datoteke.

Napadači bi mogli prilikom stvaranja zlonamjernih programa dodavati dijelove koda koji bi osiguravali zaštitu od pokušaja probijanja ključa za obnavljanje datoteka. Na primjer, napadač bi mogao omogućiti korisniku samo određen broj krivih unosa ključa za dekriptiranje prije potpunog uništenja datoteka.

Osim povećanja stvaranja i korištenja programa za *online* ucjene, očekuje se i porast trgovanja ovakvim proizvodima. Prema izvješću sigurnosnog istraživača Dancho Dancheva (http://news.softpedia.com/newsPDF/SMS-Ransomware-for-Sale-on-the-Russian-Black-Market-112888.pdf), *ransomware* programi već su dostupni na „crnom tržištu". Radi se o inačici koja se temelji na ucjenama putem SMS poruka, a početna cijena je samo $10. Za dodatnih $5 moguće je dobiti inačicu koju napadač može konfigurirati te koju mnogi antivirusni alati ne mogu detektirati. Potpuni programski kod ovakvog zlonamjernog programa moguće je dobiti za nešto veći novčani iznos od $50.

7. Zaključak

Iako je Internet marketing široko raširen u raznim djelatnostima, korisnici internetskih usluga najčešće nisu svjesni svih opasnosti koje donosi njihova uporaba. Kao jedan noviji oblik prijetnji javljaju se *online* ucjene u kojima napadači koriste neopreznost i neznanje korisnika kako bi ostvarili profit. Najčešće se koriste raznim zlonamjernim programima, poput *scareware* i *ransomware* programa. Prvi oblik programa služi za zastrašivanje korisnika kako bi preuzeli lažne antivirusne alate, ali ne nanosi štetu računalnom sustavu. Drugi spomenuti programi obično uključuju tehnike koje zaključavaju ili kriptiraju datoteke na sustavu te pri tome korisnici mogu trajno izgubiti važne podatke.

Razvojem tehnologije napadači poboljšavaju tehnike korištene u ovakvim zlonamjernim programima. Trenutno postoje inačice zlonamjernih programa koje koriste sofisticirane kriptografske algoritme (RSA s ključem duljine 1024 bita – npr. „PGPCoder") čije je dekriptiranje nemoguće u stvarnom vremenu čak i računalnim stručnjacima. Postoji mogućnost da će napadači razviti toliko napredne programe da korisnici neće imati drugi izbor osim isplate traženih novčanih iznosa.

Ipak, postoje neke metode koje osiguravaju određenu razinu zaštite. Korištenjem osvježenih inačica operacijskog sustava, ugradnjom vatrozida i IDS sustava zaštite te uporabom antivirusnih alata, osigurava se osnovna razina zaštite. Kao dodatna zaštita korisnicima se savjetuje uporaba blokiranja prozora koji se pokreću prilikom pregleda sadržaja web stranica te izrada sigurnosnih kopija važnijih datoteka.

8. Reference

[1] Internet marketing, http://en.wikipedia.org/wiki/Internet_marketing, lipanj, 2009.

[2] Etika poslovanja, http://en.wikipedia.org/wiki/Marketing_ethics, lipanj, 2009.

[3] Zlonamjerni programi, http://en.wikipedia.org/wiki/Malware, lipanj, 2009.

[4] Prevare klikom, http://en.wikipedia.org/wiki/Click_fraud, lipanj, 2009.

[5] Scareware, http://en.wikipedia.org/wiki/Scareware, lipanj, 2009.

[6] Iskakajuće poruke, http://en.wikipedia.org/wiki/Pop-up, lipanj, 2009.

[7] Randsomware, http://en.wikipedia.org/wiki/Ransomware_(malware), lipanj, 2009.

[8] Cryptovirology, http://en.wikipedia.org/wiki/Cryptovirology, lipanj, 2009.

[9] Qinyu Liao, RANSOMWARE: A GROWING THREAT TO SMES, The University of Texas at Brownsville and Texas Southmost College, Brownsville, http://www.swdsi.org/swdsi08/paper/SWDSI%20Proceedings%20Paper%20S400.pdf

[10] Zaštita, http://www.scambusters.org/ransomware.html, lipanj, 2009.

[11] New Trojans: give us $300, or the data gets it!, http://arstechnica.com/security/news/2007/07/new-trojans-give-us-300-or-the-data-gets-it.ars, 2007.

[12] New ransomware locks PCs, demands premium SMS for removal, http://blogs.zdnet.com/security/?p=3197, 2009.

[13] SMS Ransomware Threat, https://forums2.symantec.com/t5/Malicious-Code/SMS-Ransomware-Threat/ba-p/393500;jsessionid=3A2BEC4A6A5BD748AD9B41DD81F93745#A264, travanj, 2009.

[14] Vatrozid, http://en.wikipedia.org/wiki/Firewall_(networking), lipanj, 2009.

[15] Pop-up prozori, http://en.wikipedia.org/wiki/Pop-up, lipanj, 2009.

[16] IDS sustavi, http://en.wikipedia.org/wiki/Intrusion-detection_system, lipanj, 2009.

[17] Sigurnosne kopije, http://en.wikipedia.org/wiki/Backup, lipanj, 2009.

[18] Slika diska, http://en.wikipedia.org/wiki/Disk_image, lipanj, 2009.