HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

PARAZITSKI PROGRAMI

CCERT-PUBDOC-2002-12-11

CARNet CERT u suradnji s LS&S

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

Rezultat toga rada ovaj je 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

Parazitski programi su nezavisni programi koji se distribuiraju i instaliraju sa aplikacijama koje korisnici instaliraju i upotrebljavaju u svom radu.
Internet marketing kompanije sve više i više koriste parazitske programe koji se instaliraju zajedno sa legitimnim aplikacijama. Na taj način kompanije mogu doći do povjerljivih informacija kao što su navike korisnika pri surfanju, korisničke datoteke, podaci o iskorištenosti diskovnog prostora i procesorskih resursa itd.
Većina takvih programa trenutno se koristi za reklamiranje, ali njihove mogućnosti su puno šire. Unutar pravila o licenciranju nekih aplikacija dobro su sakriveni paragrafi koji kompanijama omogućavaju nekontrolirani pristup korisničkim računalima. Neke kompanije idu čak toliko daleko da planiraju prodaju neiskorištenih diskovnih i procesorskih resursa drugim kompanijama.
Parazitske programe valja razlikovati od programa za dijeljenje resursa (npr. SETI Screensaver) koji su pokrenuti na korisničkim sustavima i troše računalne resurse onda kad ih korisnik ne upotrebljava.

2. Način rada

Općenito se parazitski programi mogu podijeliti u 3 osnovne skupine:

- *Adware*,
- *Spyware*,
- *Stealth* mreže.

Većina tih programa instalira se prilikom instalacije aplikacije koje je korisnik kupio ili skinuo na svoj sustav.

2.1. Adware

Vjerojatno najpoznatiji parazitski programi su *adware* programi. Najpoznatiji i najuočljiviji takvi programi su oni koji prikazuju reklame na raznim web stranicama koje korisnik posjećuje. Te reklame su namjerno umetnute od strane vlasnika web stranica koje se posjećuju i obično se sastoje od nekoliko linija HTML ili JScript kôda. Općenito vlasniku stranice plaća se mala količina novca za svaku osobu koja sa vlasnikove stranice dođe na stranicu kompanije koja se reklamira. Takvi linkovi su obično standardni HTML <img> tagovi. Osim prikaza reklame ti tagovi često šalju i informacije o stranici koja se pregledava, tako da reklama koja se prikazuje u *browseru* cilja na ono što bi korisnika moglo interesirati, obzirom na sadržaje koje pregledava na stranici koja sadrži reklamu.
Zajedno sa zahtjevom za reklamom, korisnikov *browser* reklamnom poslužitelju eventualno šalje i kolačiće (*engl. cookie*) koje je taj poslužitelj ranije poslao korisniku. Ti kolačići služe za identifikaciju korisnikovog računala reklamnoj kompaniji. Oni ne identificiraju korisnika, osim ukoliko on nije dao svoje osobne podatke. Ti kolačići se također koriste da bi reklame koje se prikazuju što bolje odgovarale korisničkom profilu generiranom prema stranicama koje je korisnik posjetio.
Varijanta ovakvog načina sakupljanja informacije jesu slike veličine samo jednog pixela. Takva slika ne sadrži nikakve reklame nego se isključivo koristi za prikupljanje informacija o korisnikovim navikama.
Ovakvi *adware* programi često podrazumijevaju i *pop-up* prozore koji sadrže reklame prilikom posjete određenim web stranicama. Takve web stranice sadrže jednostavne JScript *applete* koji otvaraju novi prozor i umeću reklamu u njega.
Aktivni *adware* programi su inačica *adware* programa koji se sastoje od programa koji je pokrenut na sustavu i koji prima reklame (npr. KaZaA Media Desktop), te ih prikazuje kada je neki uvjet ispunjen. Ti programi često imaju arhivu reklama pohranjenu na računalu, tako da se reklame mogu prikazivati neovisno o tome da li je korisnik *online* ili *offline*. Također, takvi programi prilikom spajanja na Internet osvježavaju svoju bazu reklama, te ih tako osvježene ponovno prikazuju.

2.2. Spyware

Iako se prema načinu dolaska do informacija o navikama korisnika i njihovim afinitetima u želji za prikazom ciljanih reklama *spyware* programi ne razlikuju od *adware* programa, oni predstavljaju posve drugu grupu parazitskih programa.

Dok *adware* programi prema sadržaju posjećene stranice prikazuju odgovarajuću reklamu, *spyware* programi aktivno nadgledaju sve korisnikovo surfanje i šalju izvješća marketing poslužitelju. Općenito *spyware* da bi došao do informacija o posjećenim stranicama pregledava *history* datoteke, *Favourites* liste, *Temporary Internet Files* direktorije, te kolačiće. Sve te informacije se prikupljaju i šalju *spyware* poslužitelju. Nakon toga *spyware* program nastavlja prikupljati informacije o ostalim stranicama koje korisnik posjećuje.
Općenito, *spyware* je svaki programski paket koji koristi korisnikove računalne ili mrežne resurse bez njegovog znanje ili eksplicitne dozvole.

2.3. *Stealth* mreže

Stealth mreže su mreže računala koje dijele specifične vrste informacija. Općenito, to su *peer-to-peer* mreže koje služe za dijeljenje datoteka. Na taj način datoteke su pohranjene na mnogim različitim računalima, a prilikom pretrage upit se prosljeđuje od jednog računala prema drugom dok se datoteka ne pronađe.
Te mreže koriste se standardnom mrežnom infrastrukturom za komunikaciju, ali operativno se ponašaju kao nezavisne mreže. *Stealth* mreže mogu se koristiti za pohranjivanje datoteka i zadataka za izvršavanje na sustavima drugih korisnika.
Da bi takve mreže bile operativne na svakom korisničkom računalu mora biti instalirana odgovarajuća aplikacija koja to računalo čini dijelom *stealth* mreže.

2.4. *Browser Helper* objekti

Browser Helper objekti (*engl. Browser Helper Objects – BHO*) predstavljaju drugi način na koji *adware*, *spyware* ili programi za *stealth* mreže mogu postati dio korisnikovog sustava. BHO su u osnovi add-in programi za Internet Explorer koji se pokreću i aktivni su kad god se pokreće Internet Explorer. BHO su ustvari `.dll` biblioteke i sadrže izvršni kôd, te mogu funkcionirati isto kao i normalni programi. Nedostatak je u tome da ne postoji način da se unutar Internet Explorer-a vidi koji BHO se pokreću, te da se njihovo pokretanje onemogući ili da se oni odstrane.
Za detekciju BHO objekata potrebno je pronaći njihove potpise u *registry* datoteci. Trenutno instalirani BHO objekti su registrirani u podključevima sljedećeg *registry* ključa:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\`
Podključevi su imenovani prema CLSID identifikaciji pojedinog BHO. CLSID je jedinstveni broj koji identificira pojedinu izvršnu datoteku. Glavni nedostatak u ovom slučaju je taj da ne postoji jednostavni način određivanja koji BHO su instalirani ili onemogućiti njihovo instaliranje.

3. Opasnosti parazitskih programa

Parazitski programi koji trenutno postoje uglavnom su više naporni za korisnike, nego što predstavljaju opasnost za privatnost podataka. Koliko je poznato, današnji parazitski programi ne uzrokuju nikakvu štetu, no ne može se garantirati da će tako biti i u budućnosti. Općenito, parazitskim programima je dozvoljen pristup svim resursima sustava. Ukoliko se to uzme u obzir lako je zaključiti da su zlonamjerne mogućnosti parazitskih programa vrlo široke. Neke od njih mogu biti sljedeće:

- slanje korisničkih podataka drugim poslužiteljima,
- nadgledanje e-mail poruka i otkrivanje njihovog sadržaja,
- slanje lažnih e-mail poruka,
- otvaranje *backdoor* rupa koje napadači mogu iskoristiti sa udaljenih lokacija,
- omogućavanje korištenja računalnih resursa,
- promjena i/ili oštećivanje korisničkih i sistemskih datoteka.

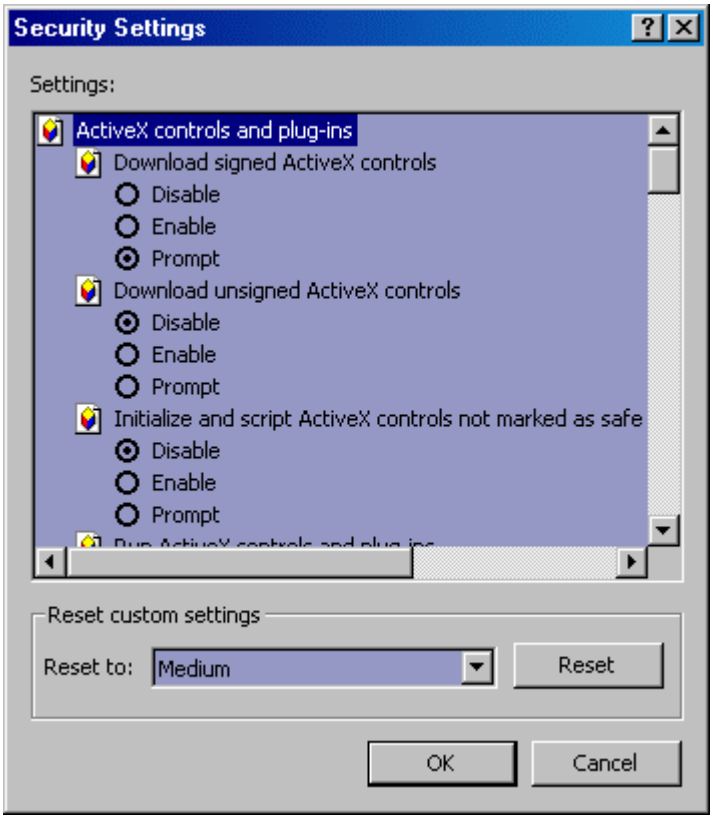
4. Detekcija i uklanjanje parazitskih programa

Detekcija parazitskih programa nije trivijalan posao jer su ti programi često sakriveni na neupadljivim mjestima, a njihovo pokretanje je povezano sa naoko bezazlenim programima. Također, neki besplatni programi neće raditi ukoliko su njihove komponente koje se koriste za reklamiranje onemogućene.

Neki parazitski programi koriste Web3000 paket koji zamjenjuje originalnu `wsock32.dll` biblioteku za dinamičko povezivanje. Takvi paketi moraju biti pažljivo uklonjeni, a `wsock32.dll` biblioteka obnovljena u procesu deinstalacije.
Uklanjanje parazitskih programa razlikuje se od programa do programa i može uključivati uklanjanje programa isto kao i uklanjanje pojedinih *registry* ključeva. Ponekad uklanjanje aplikacije koja je instalirala parazite uklanja i same parazitske programe, no često to nije slučaj.
U nastavku dokumenta dani su neki postupci kojima se može olakšati proces detekcije i eliminacije parazitskih programa.

4.1. Postavke Internet Explorer-a

Najefikasniji način borbe protiv parazitskih programa jest onemogućavanje njihove instalacije. Neki od tih programa mogu se instalirati prilikom instalacije aplikacije koja se želi koristiti, ali drugi se instaliraju prilikom pristupa određenom sadržaju na nekim web stranicama. Da bi se onemogućila takva instalacija potrebno je onemogućiti skidanje i instaliranje nepotpisanih ActiveX kontrola unutar Internet Explorer-a (*Tools* -> *Internet Options* -> *Security* -> *Internet Zone* -> *Custom* -> *Download unsigned ActiveX control* podesiti na "*Prompt*" ili "*Disable*").



Slika 1: *Prikaz sigurnosnih postavki Internet Explorer-a vezanih uz ActiveX kontrole*

4.2. Sysdiff

Sysdiff je program koji je dio Windows 2000 Resource Kit-a. Predviđen je za pregled konfiguracije sustava, odnosno određivanja koje su datoteke dodane, uklonjene i koje promjene *registry* datoteke su se dogodile prilikom instalacije pojedinog programa. Alat je potrebno pokrenuti prije i nakon instalacije pojedinog programa da bi se vidjele promjene koje je instalacija napravila u sustavu.

4.3. Oh

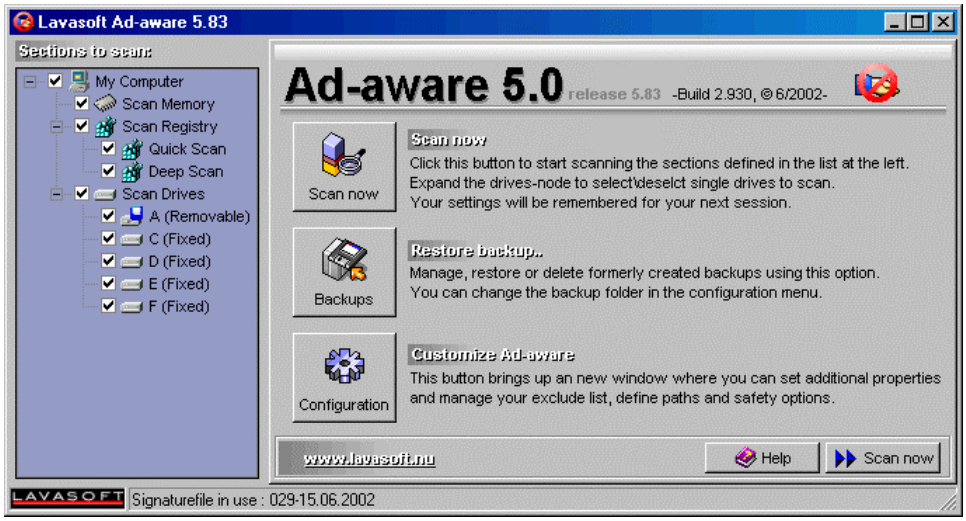
Oh alat je također dio Windows 2000 Resource Kit grupe alata. Potrebno ga je pokrenuti i nakon toga napraviti restart računala. Nakon što se pokrene sljedeći puta alat će dati popis svih otvorenih

objekata. Korištenjem `-t File` opcije moguće je vidjeti popis svih datoteka otvorenih od strane nekog procesa. Taj popis omogućava pregled datoteka koje pojedini programi otvaraju.
Tipičan prikaz otvorenih datoteka od strane Internet Explorer-a izgledao bi na sljedeći način:

```
C:\PROGRA~1\RESOUR~1>oh -p 1356 -t file
0000054C IEXPLORE.EXE   File           0060 \Documents and
Settings\hsegudov.LSS\Desktop
0000054C IEXPLORE.EXE   File           0138 \Documents and
Settings\hsegudov.LSS\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
0000054C IEXPLORE.EXE   File           014c \Documents and
Settings\hsegudov.LSS\Cookies\index.dat
0000054C IEXPLORE.EXE   File           0154 \Documents and
Settings\hsegudov.LSS\Local Settings\History\History.IE5\index.dat
0000054C IEXPLORE.EXE   File           021c \ROUTER
```

4.4. AdAware

AdAware (http://www.lavasoft.de) je program koji se sastoji od dvije komponente: AdAware komponente, koja služi za detekciju i uklanjanje parazitskih programa, te RefUpdate komponente koja automatskih skida i osvježava popis poznatih parazitskih programa. Program je besplatan za nekomercijalne korisnike.
Program radi na načelima antivirusnih programa po tome što koristi popis potpisa poznatih *adware* i *spyware* programa. Na taj način vrši se detekcija i uklanjanje. Također, program radi *backup* uklonjenih komponenata tako da ih se može obnoviti ukoliko dođe do neželjenih pojava u sustavu nakon njihovog uklanjanja. Zbog pojavljivanja novih *adware* i *spyware* programa, popis potpisa mora se redovito osvježavati, što je i svrha RefUpdate komponente.



Slika 2: *Lavasoft Ad-aware aplikacija*

4.5. Spybot Search and Destroy (SSD)

Spybot Search and Destroy (SSD) program trenutno je u procesu beta testiranja. Sličan je AdAware programu jer koristi potpise poznatih parazitskih programa. Popis potpisa biti će uključen u sam program i neće se moći osvježavati bez osvježavanja cijelog programa. SSD će imati i dodatne opcije kao npr. mogućnost umetanja lažnih *adware* i *spyware* programa, tako da programi koji inače ne rade bez tih svojih komponenti mogu nastaviti sa radom.

4.6. BHOCop

BHOCop je alat za detekciju i uklanjanje *Browser Helper* objekata (BHO). Detekcija BHO vrši se provjeravanjem *registry* datoteke, odnosno *registry* ključeva gdje su BHO pohranjeni. U slučaju detekcije BHO se onemogućava uklanjanjem ključa, dok se sam programski kôd ne uklanja. Alat također ima *backup* datoteku iz koje je moguće obnoviti sve uklonjene ključeve. Također je moguće pokretanje alata u *startup* proceduri i redovno uklanjanje BHO koji se automatski postavljaju iz drugog programa.

5. Zaključak

Parazitski programi kao što su aktivni *adware* i *spyware* programi, isto kao *stealth* mreže su programi koje bi trebalo što više izbjegavati. U slučajevima kada su u pitanju sustavi koji sadrže povjerljive informacije takve programe bi trebalo u potpunosti eliminirati.

U ovom trenutku parazitski programi, osim toga što mogu ometati korisnike u radu prikazivanjem neželjenih reklama, u načelu nisu toliko štetni. No već u bliskoj budućnosti moguće su razne mogućnosti zlouporabe, od kojih su neke opisane i ovim dokumentom.

Lako je moguće da parazitski programi postanu prijetnja korisnicima na način koji danas to predstavljaju računalni virusi. Moguće je očekivati pojavu i široku uporabu programske podrške za detekciju i uklanjanje parazitskih programa. Drugi pristup pak može biti dodavanje potpisa tih programa u baze potpisa antivirusnih programa. U ovom trenutku postoji nekoliko programa koji prilično uspješno mogu detektirati i uklanjati parazitske programe koji se danas pojavljuju.