HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Praćenje unosa znakova preko tipkovnice

CCERT-PUBDOC-2007-11-211

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

Keylogger je program ili uređaj koji služi za praćenje unosa znakova preko tipkovnice. Katkad se još naziva i *keystroke logger, key logger* ili *system monitor*. Takvi alati prate i bilježe svaku tipku koju korisnik pritisne. Moguće ih je podijeliti u dvije skupine:

- alati koji dolaze u obliku programskih paketa i
- uređaji koji pripadaju sklopovlju računala.

Keylogger alati mogu imati pozitivan učinak na sigurnost računalnog sustava te služiti kao dodatak već instaliranim sigurnosnim programima ili mogu predstavljati veliku sigurnosnu ranjivost za individualni sustav ili za cijelu računalnu mrežu.

Glavne metode koje se koriste za tzv. *cyber* prijevare (eng. *cyber frauds*) su:

- *keylogger* alati,
- tzv. *phishing* prijevare – prijevare podmetanjem lažnih poruka elektroničke pošte ili lažnih web stranica i
- razne metode nagovaranja i manipuliranja korisnika na odavanje povjerljivih podataka ili poduzimanja nekih akcija koje pogoduju zlonamjernim napadačima (eng. *social engineering*).

Korisnici svjesni ranjivosti vlastitog sustava mogu se zaštititi od *phishing* napada ignoriranjem određenih poruka elektroničke pošte i pažnjom pri upisu osobnih podataka na web stranicama koje to zahtijevaju. Mnogo je teže zaštititi sustav od napada *keylogger* alatima jer je često nemoguće znati je li *keylogger* instaliran na ranjivom računalu ili nije pa je jedina moguća mjera zaštite upotreba prikladnih sigurnosnih rješenja.

2. Općenito o alatima za praćenje unosa znakova preko tipkovnice (eng. *keylogger*)

Glavna ideja alata za praćenje unosa znakova preko tipkovnice jest uključivanje u lanac događaja između pritiska tipke na tipkovnici i prikaza znaka na ekranu. To je moguće postići postavljanjem video nadzora, podmetanjem prislušnog uređaja u tipkovnicu ili korištenjem samog računala za presretanje unosa znakova, prepisivanjem upravljačkih programa tipkovnice te upravljačkih programa za obavljanje posebnih funkcija tipkovnice (eng. *filter driver*), presretanjem funkcija jezgre operacijskog sustava (npr. zamjenom adresa u sistemskim tablicama, manipuliranjem programskim kodom funkcija, itd.), presretanjem DLL (eng. *Dynamic-link library*) funkcija u korisničkom načinu rada i konačno, zahtijevanjem podataka od tipkovnice uporabom standardnih dokumentiranih metoda.
Kao što je već spomenuto u uvodu, *keylogger* alati dijele se u dvije kategorije, a to su sklopovski uređaji i programski paketi. Sklopovski uređaji su obično male naprave koje se postavljaju u tipkovnicu, žicu od tipkovnice ili u računalo, dok se programski paketi obično sastoje od programa koji prate i bilježe pritiske tipki na tipkovnici.

2.1. Sklopovski *keylogger* alati

Sklopovski *keylogger* je uređaj koji se umetne između tipkovnice i priključka za tipkovnicu na matičnoj ploči računala. Ovakav način upotrebe *keylogger* uređaja zahtijeva ugradnju u tajnosti, što može predstavljati određene poteškoće za napadača, pogotovo u prostoru u kojem ljudi borave tijekom cijelog dana. Prednost korištenja ovakvih uređaja jest izbjegavanje potrebe za manipulacijom procesima operacijskog sustava, što bitno smanjuje vjerojatnost detekcije. U nastavku su navedene neke prednosti i nedostaci *keylogger* uređaja.
Prednosti:

- nema potrebe za posjedovanjem određenih ovlasti pri instalaciji uređaja,
- prati se i bilježi svaki unos znakova preko tipkovnice, uključujući i zaporke za BIOS (eng. *Basic Input/Output System*),
- ugradnja je jednostavna, nema potrebe za tehničkim predznanjem,
- neovisni su o operacijskom sustavu i
- ne mogu se detektirati antivirusnim programima ili bilo kojim drugim sigurnosnim programskim paketima.

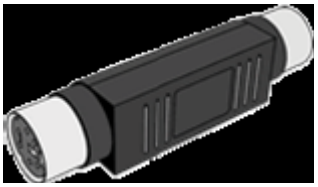
Nedostaci:

- potrebno je imati pristup sklopovlju računala,
- imaju mali kapacitet memorije za spremanje podataka i
- nemaju mogućnost zapisa vremena pojedinog pritiska tipke.

Slika 1 prikazuje tipkovnicu s integriranim *keylogger* uređajem, tzv. *KeyGhost Security Keyboard*. Tipkovnicu je moguće nabaviti kod svih proizvođača, a profesionalna SE tipkovnica ima 128-bitnu enkripciju i sposobnost pamćenja više od 2,000,000 unosa znakova.

Slika 1. Primjer tipkovnice s integriranim *keylogger*-om (KeyGhost Security Keyboard)

Slika 2 prikazuje primjer uređaja "*KeyGhost SX*" sa kapacitetom memorije 2 MB. Takav uređaj može pamtiti više od 2,000,000 pritisaka tipki na tipkovnici, a osim toga koristi i 128-bitnu enkripciju pri spremanju podataka.



Slika 2. Primjer sklopovskog *keylogger*-a (KeyGhost SX)

2.2. Programski *keylogger* alati

Keylogger kao programski paket za praćenje unosa znakova preko tipkovnice namijenjen je nadzoru ponašanja korisnika. Za razliku od sklopovskog uređaja, program može pratiti mnogo više od samih pritisaka tipki na tipkovnici. *Keylogger* program koji je instaliran na operacijskom sustavu moguće je otkriti antivirusnim alatima i drugim programskim paketima za otkrivanje sigurnosnih propusta na računalu. Još neke prednosti i nedostaci *Keylogger* programa navedene su u nastavku.

Prednosti:

- Teško ga je otkriti bez specijalnih programskih alata.
- Moguće ga je instalirati s udaljenog računala.
- Nema potrebe za sklopovljem ili uređajima pri instalaciji.
- Datoteke u koje se spremaju podaci nemaju ograničen kapacitet memorije.
- Datoteke sa zapisima pritisaka tipki moguće je preuzeti na mnogo načina, npr. putem elektroničke pošte, ftp (eng. *file transfer protocol*) prijenosa podataka ili izravnim preuzimanjem s računala s instaliranim *keylogger* programom.
- Postoje brojne vrste *keylogger* programa s velikim rasponom cijena.
- Moguće je pridružiti datum, vrijeme i korišteni program određenim unosima znakova preko tipkovnice.
- Uključuju i druge načine praćenja, kao što su snimke zaslona računala snimljene npr. svakih pet minuta.

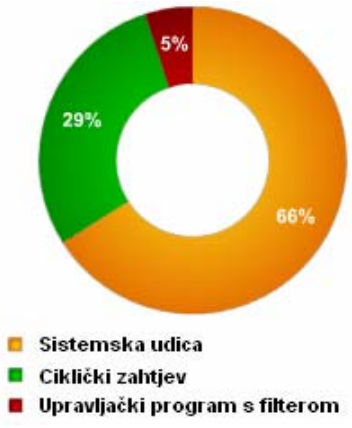
Nedostaci:

- Moguće ga je otkriti pomoću antivirusnih programa ili drugih sigurnosnih alata.
- Potrebne su određene ovlasti da bi se program mogao instalirati na sustav.
- Može narušiti normalan rad drugih programa i izazvati neočekivane pogreške ili prikaz poznatog plavog ekrana na operacijskom sustavu Windows.
- Ne pamti pritiske tipki prije pokretanja operacijskog sustava te je nemoguće na taj način zabilježiti zaporke za BIOS ili korisničko ime i zaporku za prijavu na sustav.
- Potrebni su određeno predznanje i vještina za instalaciju programa.
- Postoji mogućnost da program neće raditi te da ovisi o operacijskom sustavu.
- Potrebno je prethodno znati na koji će se operacijski sustav program instalirati.

Uobičajene metode izrade *keylogger* programa:

- postavljanje tzv. sistemske udice (eng. *system hook*) koja presreće obavijest o pritisnutoj tipki (Program se koristi već ugrađenim programskim sučeljem. Primjerice, kod Windows operacijskih sustava, *WinAPI* metodom *SetWindowsHook* za poruke poslane prozorskim procedurama.),
- postavljanje cikličkih zahtjeva za informacijama o događajima na tipkovnici (Ovakvi Windows programi koriste *WinAPI* metode *Get(Async)KeyState* ili *GetKeyboardState*. Najčešće su pisani u programskom jeziku Visual Basic, a katkad i u Borland Delphi programskom jeziku) te
- korištenje upravljačkih programa za obavljanje posebnih funkcija (eng. *filter driver*) (Izrada zahtjeva odlično poznavanje sustava, a program se obično piše u programskom jeziku C.).

Slijedi prikaz statističkih podatka o *keylogger* programima. Na grafu je prikazana raspodjela različitih vrsta *keylogger* programa:



Slika 3. Graf raspodjele učestalosti metoda korištenih za izradu *keylogger* programa

U posljednje vrijeme raste broj programa s ugrađenim sustavom za skrivanje datoteka sa zapisima o unosima znakova s tipkovnice u svrhu zaštite od detekcije antivirusnim programima. Metode koje se koriste za skrivanje datoteka su tzv. *rootkit* tehnologije - skup programa kojima je moguće sakriti tekuće procese, datoteke ili sistemske podatke od operacijskog sustava. *Keylogger* programi koriste dvije glavne *rootkit* metode:

- maskiranje u korisničkom načinu rada i
- maskiranje u administratorskom načinu rada.

Slijedeći graf prikazuje raspodjelu tehnika za maskiranje aktivnosti *keylogger* programa:

Slika 4. Graf učestalosti upotrebe načina skrivanja aktivnosti *keylogger* programa

3. Razlozi za korištenje *keylogger* alata

Neki legalni programi imaju integriranu *keylogger* funkcionalnost. Ona se koristi za pribavljanje informacija o upotrebi kombinacija tipki koje pokreću neki dio programa nad kojim su upotrijebljene (eng. *hotkeys*), a osim toga mogu se upotrijebiti i za prebacivanje između različitih shema znakova na tipkovnici (npr. *Keyboard Ninja*). Postoji mnogo programskih paketa kojima administratori mogu pratiti aktivnosti zaposlenika ili korisnicima osobnih računala dati mogućnost praćenja aktivnosti nekih udaljenih korisnika njihovih računala. Ipak, postoji tanka linija između opravdanog praćenja i špijuniranja korisnika. Legalni se programi često koriste za krađu povjerljivih korisničkih podataka, kao što su npr. zaporke.

Većina modernih *keylogger* programa ili uređaja smatra se legalnim i prodaju se na slobodnom tržištu. Razvojni programeri i trgovci nude niz primjera kod kojih je upotreba *keylogger* programa ili uređaja legalna i primjerena, uključujući:

- roditeljski nadzor - roditelji mogu pratiti što njihova djeca rade na Internetu i mogu tražiti slanje obavijesti ukoliko djeca pokušaju pristupiti web stranicama s neprimjerenim sadržajima,
- ljubomorni supružnici ili partneri mogu koristiti *keylogger* programe ili uređaje za praćenje akcija svojih partnera na Internetu, ukoliko ih sumnjiče za tzv. "virtualno varanje",
- sigurnost tvrtke - praćenje zaposlenika u smislu upotrebe računala za vlastite potrebe, ili korištenja radnih stanica nakon odrađene satnice,
- sigurnost tvrtke - upotreba *keylogger* programa ili uređaja za praćenje upisa ključnih riječi ili fraza vezanih uz komercijalne informacije koje mogu naškoditi tvrtki (materijalno ili na neki drugi način) ukoliko se takvi podaci objave,
- sigurnost (policija, vojska, zakonodavstvo) - upotreba zapisa za analizu i praćenje incidenata vezanih uz korištenje osobnih računala i
- drugi razlozi.

Ipak, upravo nabrojana opravdanja su subjektivne naravi i sve se situacije mogu riješiti na neki drugi način. Osim toga, svaki se legalni program može iskoristiti u kriminalne svrhe. Danas se *keylogger* programi i uređaji uglavnom koriste za krađu korisničkih podataka vezanih uz web sustave za plaćanje kreditnim karticama. Programeri virusa konstantno stvaraju nove trojanske konje upravo za krađu podataka kreditnih kartica. Nadalje, mnogi se *keylogger* programi skrivaju u sustavu (npr. imaju *rootkit* funkcionalnost), što ih čini pravim trojanskim konjima.

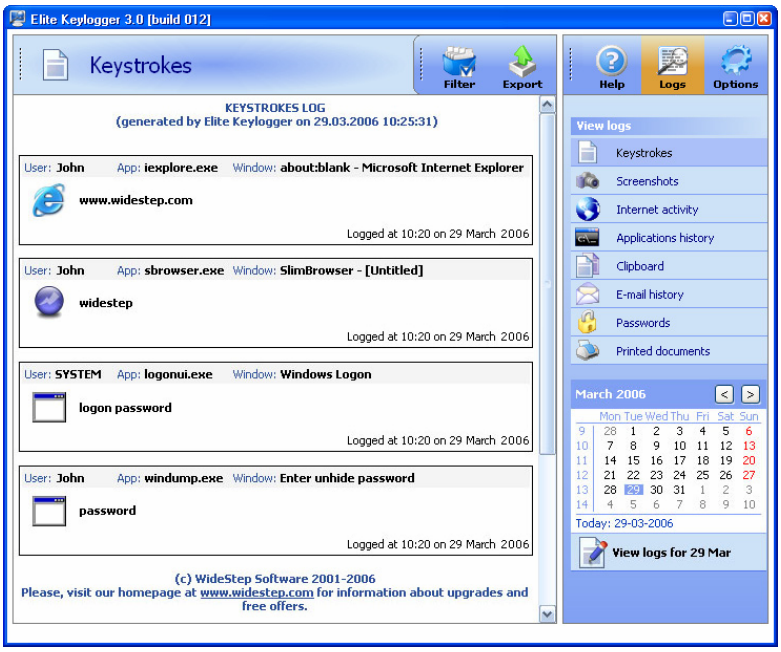
Zbog rasta popularnosti takvih zlonamjernih programa među tzv. *cyber* kriminalcima, tvrtkama koje kreiraju antivirusne programe treba biti prioritet ugradnja zaštite i otkrivanje zlonamjerno postavljenih *keylogger* programa.

3.1. Primjer *keylogger* alata

Jedan od popularnijih *keylogger* alata je *Elite Keylogger* koji ima mogućnosti praćenja i zapisivanja svakog detalja aktivnosti korisnika na osobnom računalu i Internetu. Program ima integrirane skrivene module koji prate i bilježe razgovore preko Interneta (eng. *chat*), zapisuju primljene i poslane *instant* poruke, poruke elektroničke pošte, posjećene web stranice, pritiske tipki na tipkovnici, pokrenute programe, upisane zaporke, pa čak i zaporke za prijavu na operacijski sustav Windows, korisnička imena te vrijeme kada su se prijavili na sustav, aktivnosti na radnoj površini i u međumemoriji te još mnogo toga. Osim toga, program sprema i tzv. povijest praćenih događaja, tako da korisnik može vidjeti što su njegovi članovi obitelji, susjedi, zaposlenici ili drugi korisnici radili na računalu ili još uvijek rade. *Elite Keylogger* u potpunoj tajnosti sprema zapise na lokaciju skrivenu od običnih korisnika, pri čemu su svi zapisi kriptirani.

Slijede neke funkcionalnosti koje podržava spomenuti *keylogger* alat:

- **Pamćenje unosa znakova s tipkovnice odnosno pritiska svake tipke na tipkovnici** – ima mogućnost prepoznavanja internacionalnih shema znakova te svih glavnih 2-bajtnih shema kodiranja znakova. Dodaje svakom pritisku tipke vremensku oznaku, dokumentira svaku pritisnutu tipku uključujući alfanumeričke znakove, "skrivene" znakove, kombinacije tipki kao što su *Shift, Alt, Tab, Ctrl, CTRL+ALT+DEL*, funkcijske tipke (F1-F12), *Print Screen, Scroll Lock*, čak *Num Lock* i ostale tipke koje se nalaze na tipkovnici. Podržava sve tipove tipkovnica (USB, PS/2, PCI). Slijedeća slika prikazuje kako *Elite Keylogger* čuva sve zapise o pritiscima tipki na tipkovnici:

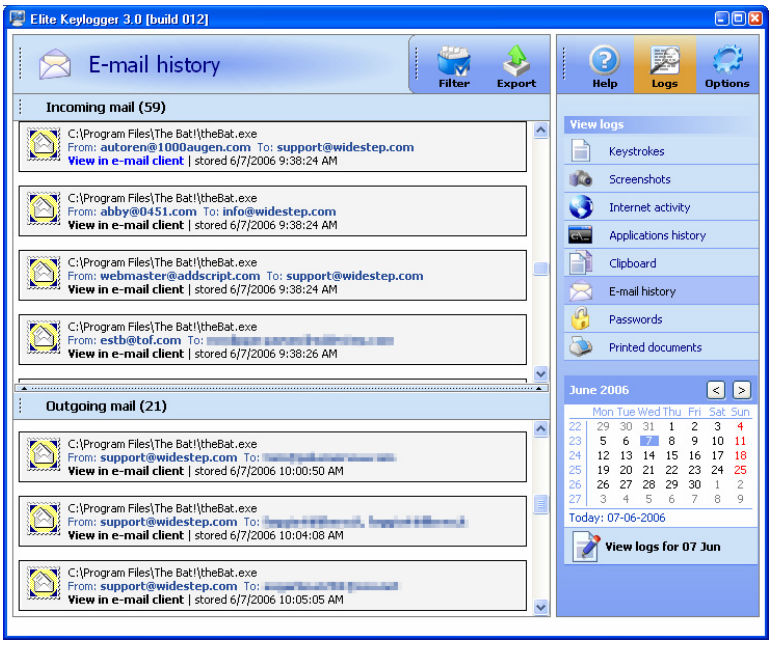


Slika 5. Grafičko sučelje *Elite Keylogger* alata i prikaz zapamćenih pritisnutih tipki

- **Skrivena instalacija** – nisu potrebne dodatne ovlasti za instalaciju upravljačkih programa niti za pokretanje alata. Također, *Elite Keylogger* ne otkriva svoju prisutnost tijekom instalacije.
- **Nevidljivost i nemogućnost detekcije –** radi skriveno što znači da nigdje ne postoji nikakva ikona, ne nalazi se u popisu procesa, popisu koji se vidi alatom *Task Manager* te popisu za uklanjanje instalacije. Neće ga otkriti čak ni *anti-keylogger* alati.
- **Čuvanje zaporki –** spomenuti program umetne u sustav svoj upravljački program jezgre, što mu omogućuje praćenje i zapisivanje zaporki za prijavu na sustav. Također pamti sve ostale upisane zaporke, pa čak i one skrivene nekim drugim znakovima osim "*" ili "●".

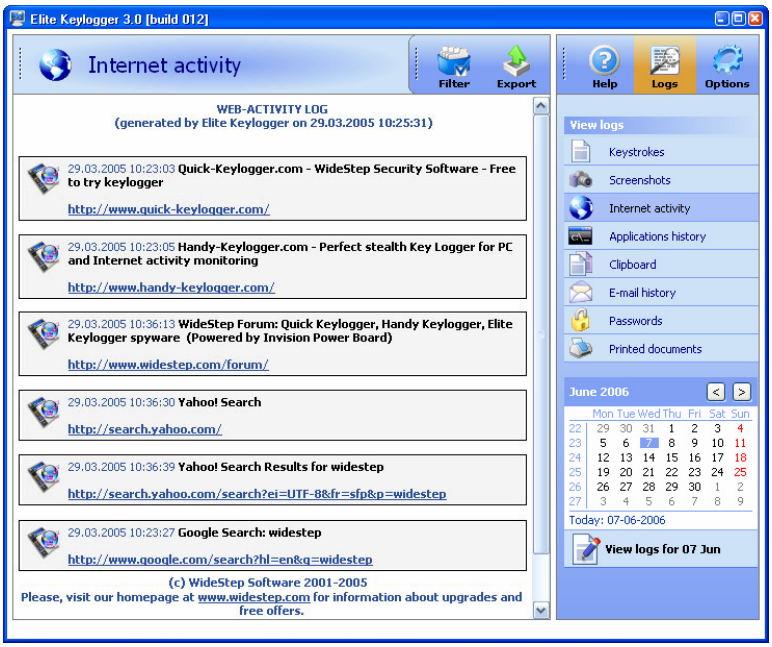
Slika 6. Prikaz zapamćenih zaporki

- **Praćenje i zapisivanje razgovora preko Interneta (eng. *chat*) –** prati sve aplikacije za razgovor preko Interneta te razgovore na web stranicama. Svakom zapisu dodaje vremensku oznaku i razvrstava zapise prema nazivu prozora kojem pripadaju.
- **Snimanje elektroničke pošte –** bilježi svaku poslanu ili primljenu poruku nekim od poznatih klijenata elektroničke pošte (*MS Exchange, The Bat!, Outlook email*). Osim toga, ima i napredne opcije praćenja elektroničke pošte pa može bilježiti i poruke s poslužitelja kao što su *Hotmail, Yahoo Mail* i *AOL Internet Email* te usluga elektroničke pošte lokalnog pružatelja usluge pristupa Internetu. Također zapisuje i sadržaj poruka, korisnički račun s kojeg su poruke primljene ili poslane te postavlja vremensku oznaku.



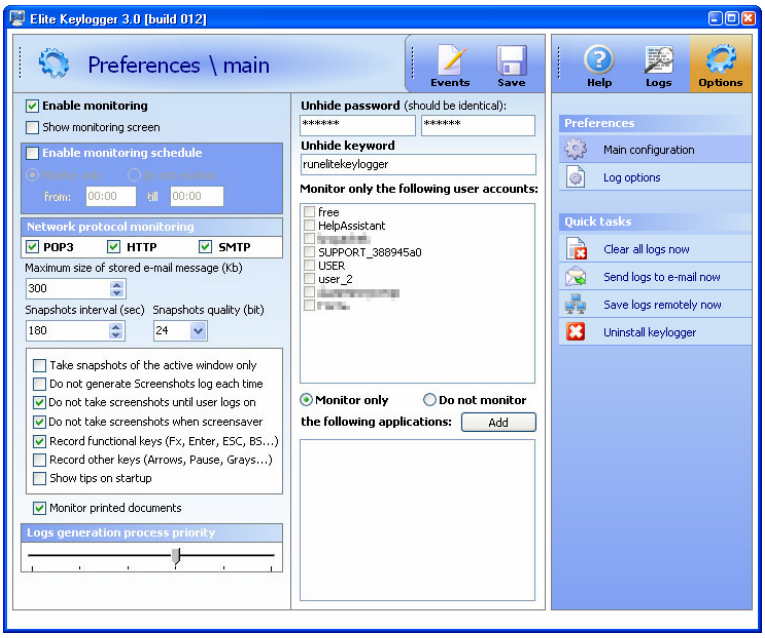
Slika 7. Pregled poslanih i primljenih poruka elektroničke pošte

- **Praćenje aktivnosti korisnika na web stranicama** – čuvaju se zapisi svih posjećenih stranica te koji je web preglednik pri tome korišten. Pamti se također i URL (eng. *Uniform Resource Locator*) adresa, naziv web stranice, vrijeme posjeta i svi korisnički detalji. Sljedeća slika prikazuje praćenje posjeta web stranicama:



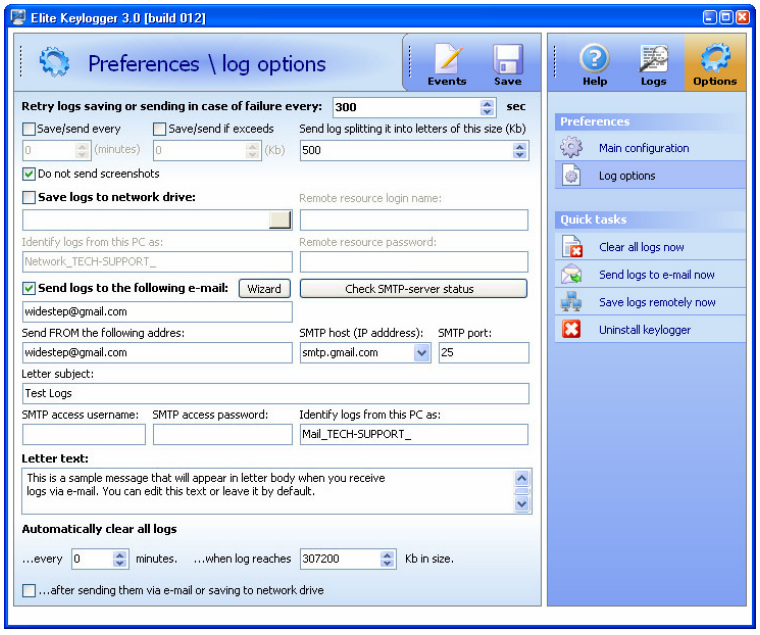
Slika 8. Praćenje posjeta web stranica

- **Snimanje zaslona ekrana –** snimanje zaslona ekrana djeluje kao nadzorna kamera, a program koristi fleksibilni sustav ključnih riječi i filtra za automatsku modulaciju frekvencije snimanja niza slika. Slike se spremaju u JPEG formatu i na svaku od njih dodaje se vremenska oznaka.
- **Praćenje sadržaja međumemorije –** ukoliko korisnik kopira neku dugu zaporku da bi ju zalijepio na određeno mjesto, ta zaporka se pamti u međuspremniku sustava ili međumemoriji. *Elite Keylogger* prati svaku promjenu sadržaja međuspremnika te čuva sve slike i tekst kopiran u sistemski međuspremnik.
- **Automatsko pokretanje –** program se pokreće prilikom pokretanja operacijskog sustava, tako da ga nije potrebno ručno pokretati.
- **Otkrivanje stanja u kojem operacijski sustav ništa ne radi (tzv. *idle* stanje) –** *Elite Keylogger* automatski pauzira praćenje aktivnosti kad je sustav u stanju *idle*. Na taj način minimizira upotrebu resursa operacijskog sustava te izbjegava snimanje velikog broja istih slika ekrana.
- **Praćenje više korisnika odjednom –** prati sve korisničke račune bez obzira jesu li zaštićeni zaporkom ili ne.
- **Zaštita pokretanja i zaustavljanja *keylogger* programa zaporkom,**
- **Kriptiranje zapisa,**
- **Automatsko brisanje zapisa –** po izboru korisnika *keylogger* alata automatski se brišu stari zapisi kada datoteka premaši predodređenu veličinu. Tako se sprečava zauzimanje previše diskovnog prostora. Također, moguće je zadati brisanje zapisa odmah nakon što su podaci poslani korisniku *keylogger* programa.



Slika 9. Napredne postavke programa

- **Obavještavanje elektroničkom poštom** – korisnik *keylogger* programa može redovito primati izvještaje u obliku poruka elektroničke pošte.
- **Pristupanje zapisima s udaljenog računala –** postoji mogućnost spremanja zapisa aktivnosti na bilo kojem računalu u mreži, a svakom se zapisu može pristupiti putem lokalne mreže (LAN) ili Interneta.



Slika 10. Postavke zapisa i slanja zapisa

- **Praćenje pokrenutih aplikacija i otvorenih prozora.**

4. Opasnosti *keylogger* alata

Konstantno se povećava broj ljudi koji koriste Internet za osobne potrebe, kao što je plaćanje računa i kupovina na web stranicama. Tvrtkama odgovara upravo takva upotreba Interneta, no to uključuje problem sigurnosti korisnika i njihovih podataka.

Upravo je zato bitno obrazovati korisnike i naučiti ih kako se osigurati od sve većeg broja zlonamjernih korisnika Interneta. Također bitno je da korisnici u potpunosti shvate kakvim se rizicima izlažu kada pokreću svoj web preglednik.

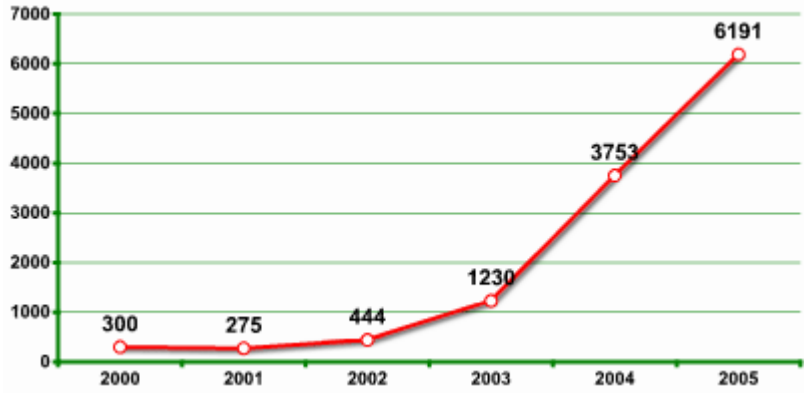
Na primjer, dobro je koristiti kriptirane poveznice (npr. HTTPS umjesto HTTP) za pristup bankovnim računima ili elektroničkoj pošti. Na taj je način prijenos privatnih informacija preko Interneta kriptiran. Međutim, vrlo je bitno uočiti da kriptiranje ne skriva podatke od računala kojem su namijenjeni. Tu do izražaja dolazi sigurnosna prijetnja koje korisnici često nisu svjesni – praćenje unosa znakova preko tipkovnice.

Jedan od poznatih nedavnih incidenata vezanih uz *keylogger* programe odnosi se na krađu više od milijun dolara sa korisničkih računa jedne od velikih Skandinavskih banaka *Nordea*. U kolovozu 2006. klijenti spomenute banke počeli su primati poruke elektroničke pošte, navodno od banke, u kojima se od njih zahtijevala instalacija programa za zaštitu od neželjenih elektroničkih poruka (eng. *antispam*) koji se nalazio u privitku. Kada je korisnik učinio što se tražilo od njega, zapravo je na računalo instalirao trojanskog konja poznatog po imenu *Haxdoor* koji bi postao aktivan kada se žrtva registrirala na Internetske usluge banke *Nordea*. Tada bi trojanski konj prikazao poruku o pogrešci sa zahtjevom za ponovnom registracijom. *Keylogger* alat bio je dio trojanskog konja i bilježio je podatke koje su unosili klijenti spomenute banke te ih je slao određenim poslužiteljima, odnosno kriminalcima. Na taj su način *cyber* zločinci došli do podataka o korisničkim računima klijenata banke te ih ispraznili. Prema autoru trojanskog konja *Haxdoor*, program su koristili i napadači na australske i mnoge druge svjetske banke.

24. siječnja 2004. zloglasni crv *Mydoom* uzrokovao je najveću epidemiju u povijesti Interneta i srušio rekord koji je postavio njegov prethodnik, crv *Sobig*. Crv je koristio metode tzv. socijalnog inženjeringa (eng. *social engineering*) i organizirao napade uskraćivanja usluga (eng. *Denial of Service – DoS*) na www.sco.com te je stranica bila nedostupna ili nestabilna sljedećih nekoliko mjeseci. Crv je za sobom ostavio trojanskog konja na zaraženom računalu, a to računalo postalo je početna točka nove zaraze modificiranom inačicom crva. Činjenica koja se nije spominjala u javnosti jest da je crv je imao funkcionalnost praćenja unosa znakova sa tipkovnice u svrhu krađe brojeva kreditnih kartica.

Postoji još mnogo primjera zlouporabe *keylogger* programa, a najviše financijskih krađa izvedeno je pomoću *keylogger* alata jer su oni najpouzdanije rješenje za dolazak do , inače skrivenih, osjetljivih informacija.

U jednom od izvještaja tvrtke *VeriSign* piše da se unazad nekoliko godina zbiva nagli porast broja zlonamjernih programa koji imaju funkcionalnost praćenja unosa znakova sa tipkovnice.



Slika 5. Prikaz rasta broja zlonamjernih programa s *keylogger* funkcionalnosti (izvor: *iDefense*, tvrtka *VeriSign*)

Jedan od izvještaja tvrtke *Symantec* pokazuje da skoro 50% zlonamjernih programa, koje su otkrili tvrtkini analitičari tijekom prošlih godina, ne predstavljaju izravnu prijetnju računalima, ali se koriste za skupljanje osobnih korisničkih podataka.

4.1. *Haxdoor* – primjer rada *keylogger* alata

Haxdoor služi napadačima kao stražnji ulaz u sustav, a ima i *rootkit* mogućnosti tako da može sakriti svoju prisutnost, procese i datoteke od sustava kojeg je inficirao. Jedini način otkrivanja spomenutog programa jest uporaba antivirusnih alata koji koriste upravljačke programe jezgre operacijskog sustava ili *rootkit* detektora, kao što je F-Secure BlackLight.
Haxdoor se može koristiti za špijuniranje i prema nekim izvještajima napadači su ga koristili za krađu podataka vezanih uz bankovne račune (korisnička imena, zaporke) te za pljačku banke *Nordea*.
Kao stražnji ulaz u sustav pokreće se datoteka CMD.EXE koja potajno kopira sedam datoteka u sistemski direktorij operacijskog sustava Windows:

- cm.dll,
- draw32.dll,
- hm.sys,
- memlow.sys,
- vdnt32.sys,
- vtd_16.exe i
- wd.sys.

Ove datoteke pokreću se tek nakon ponovnog pokretanja računala. Kada je otvoren stražnji ulaz u sustav sve su datoteke koje *Haxdoor* koristi skrivene. Štoviše, program pokušava ubaciti svoj kod u *Windows Explorer* proces te skriva procese *Explorer.exe* i *Winlogon.exe*.
Proces *vtd_16.exe* je dio Windows procesa CMD.EXE i on se pokreće za odvraćanje pozornosti. Ime programa za stražnji ulaz je CMD.EXE i on se pokreće kao interpreter naredbi u svrhu skrivanja zlonamjernih aktivnosti.
Datoteke "cm.dll" i "draw32.dll" su identične i one predstavljaju glavnu komponentu *Haxdoor* programa. U tzv. *Registry* zapisnik operacijskog sustava Windows dodaje se *Winlogon Notification* zapis:

[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\draw32]

To omogućava otvaranje stražnjih vrata u sustav, odnosno pokretanje zlonamjernog programa prilikom prijave korisnika na sustav. Zlonamjerno oblikovani programi rijetko koriste ovakav način pokretanja.
Haxdoor je moćan program i može se koristiti za krađu zaporki. Prema konfiguracijskim podacima koji su u njemu pronađeni, zaključuje se da može preuzeti podatke o korisničkim imenima i zaporkama od različitih banaka i sustava plaćanja na Internetu:

- alpha.gr,
- authorize,
- banc,
- bank,
- banq,
- Barclays,
- business,
- cdb,
- citi,
- coopcb,
- fbme,
- gold,
- halifax,
- HSBC,
- ikobo,
- merchant,

- moneybookers,
- sgcyprus,
- trade i
- VeriSign.

Uza sve spomenuto, program je moguće iskoristiti za krađu sljedećih podataka:

- POP3 zaporke,
- POP3 imena poslužitelja,
- POP3 korisničkog imena,
- IMAP zaporke,
- IMAP imena poslužitelja i
- IMAP korisničkog imena.

Zlonamjerno oblikovan program može se i poigrati s korisnikom, pa tako nekad otvara i zatvara ladicu CD-ROM uređaja.

4.2. Načini širenja *keylogger* programa

Keylogger programi šire se kao i svi ostali zlonamjerni programi, uz iznimku slučaja kada ljubomorni supružnik ili partner kupi i instalira takav program na računalo partnera ili kada se koriste u sigurnosne svrhe. Najčešći načini širenja su sljedeći:

- instalacija prilikom otvaranja datoteke iz privitka elektroničke poruke,
- instalacija prilikom pokretanja datoteke iz direktorija sa slobodnim pristupom preko P2P mreže,
- instalacija preko web stranice koja zloupotrebljava sigurnosne propuste web preglednika gdje se program automatski pokreće kad korisnik posjeti web stranicu i
- instalacija uz pomoć drugih zlonamjernih programa, koji se već nalaze na ranjivom računalu.

5. Zaštita od *keylogger* programa

Većina antivirusnih tvrtki već je dodala poznate *keylogger* programe u svoje baze podataka pa se tretiraju kao i svi ostali zlonamjenro oblikovani programi. Dakle, preporuča se instalacija antivirusnog programa i redovito obnavljanje njegove baze podataka. Međutim, većina antivirusnih programa klasificira *keylogger* programe kao potencijalno zlonamjerne ili potencijalno nepoželjne programe, tako da bi korisnici trebali provjeriti otkriva li njihov antivirusni alat, s izvornim postavkama, ovakvu vrstu programa. Ukoliko to nije slučaj, potrebno je namjestiti postavke tako da se osigura zaštita od većine poznatih *keylogger* programa.

Slijedi pregled nekih metoda zaštite od nepoznatih *keylogger* programa ili alata namijenjenih točno određenim operacijskim sustavima.

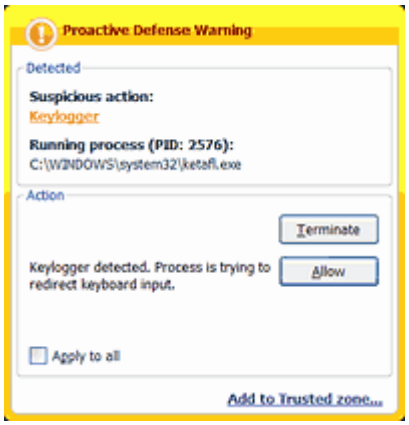
Kako je glavni cilj *keylogger* programa preuzeti povjerljive podatke (brojeve bankovnih kartica, zaporke, itd.), logični načini zaštite su:

1. korištenje jednokratnih zaporki ili dvokoračne autentikacije,
2. korištenje sustava sa proaktivnom zaštitom dizajniranom upravo za detekciju *keylogger* programa i
3. korištenje virtualne tipkovnice.

Uporabom jednokratnih zaporki moguće je smanjiti gubitke ukoliko napadač presretne unesenu zaporku. Jednokratne zaporke vrijede samo jedanput i njihova je valjanost vremenski ograničena. Čak i u slučaju da napadač presretne jednokratnu zaporku, neće je moći iskoristiti za preuzimanje i pristup povjerljivim podacima.

Bankovni sustavi širom Europe, Azije, Sjedinjenih Američkih Država i Australije koriste generatore jednokratnih zaporki. Na primjer, vodeća banka *LLoyds TSB*, koristi generatore zaporki još od studenog 2005. U ovom slučaju tvrtka je morala potrošiti mnogo novca za nabavku i distribuciju generatora zaporki svojim klijentima, a trebala je i razviti ili kupiti prateći programski paket.

Financijski isplativije rješenje jest upotreba proaktivne zaštite na klijentskoj strani koja može upozoriti korisnika na pokušaje instalacije *keylogger* programa.



Slika 6. Proaktivna zaštita protiv *keylogger* alata antivirusnim programom *Kaspersky Internet Security*

Glavni nedostatak ove metode jest potreba interakcije antivirusnog programa s korisnikom gdje on mora odlučiti koju akciju poduzeti. Ukoliko korisnik nema dovoljno iskustva, može donijeti pogrešnu odluku i nesvjesno dozvoliti instalaciju *keylogger* programa. Međutim, ako se razviju sigurnosni programi koji smanjuju sudjelovanje korisnika u takvim odlukama, tada postoji mogućnost da *keylogger* programi izbjegnu detekciju zbog nedovoljno rigorozne sigurnosti. Ako su pak postavke previše ograničavajuće, tada će biti blokirani i legalni korisni programi koji sadrže funkcionalnost praćenja unosa znakova preko tipkovnice.

Neke pametnije inačice sigurnosnih programskih paketa mogu raditi i bez antivirusnih alata, kao što su *AD-Aware* ili *Spy-Sweeper*. Oni koriste označavanje zastavicama. Još je gori slučaj sklopovskih *keylogger* uređaja jer ih antivirusni programi ne mogu detektirati. Programski paketi kao što su *SpyCop* i *SnoopFree* dizajnirani su specifično za detekciju *keylogger* programa.

Konačna metoda koja se može koristiti kao zaštita protiv *keylogger* programa i uređaja jest upotreba virtualne tipkovnice. Virtualna tipkovnica je program koji prikazuje tipkovnicu na zaslonu ekrana, a tipke se pritišću klikovima miša na određene znakove.

Ideja virtualne tipkovnice nije nova, operacijski sustav Windows dolazi s takvom tipkovnicom i moguće ju je pokrenuti na sljedeći način: *Start > Programs > Accessories > Accessibility > On-Screen Keyboard.*

Slika 7. Primjer virtualne tipkovnice operacijskog sustava Windows

Ipak, virtualne tipkovnice nisu baš popularan način nadmudrivanja *keylogger* programa i uređaja. One nisu dizajnirane da služe kao zaštita od *cyber* prijetnji, već kao alat za pomoć onesposobljenim osobama. Neki zlonamjerno oblikovani program lako će presresti podatke unesene preko virtualne tipkovnice. Kako bi bilo moguće koristiti virtualnu tipkovnicu kao zaštitu protiv *keylogger* programa i uređaja, ona bi trebala biti posebno prilagođena sprečavanju presretanja unesenih ili poslanih podataka.

6. Zaključak

Praćenje unosa znakova preko tipkovnice jest zadiranje u privatnost korisnika, a uz to je, u određenim slučajevima, i ilegalno. Ipak, ova spoznaja, sama za sebe, ne čini alate namijenjene praćenju unosa znakova manje korištenim, a pogotovo ih ne čini nedostupnima. Zato je u ovom trenutku ključno korisnike naoružati znanjima o takvim programima i uputiti ih na najbolja rješenja. Potrebno ih je, primjerice, navesti na promišljanje prije nego se upuste u korištenje javnih računala za pristup privatnim podacima.

Na web stranici *Keyloggers*.com postoji opsežan popis *keylogger* programa i uređaja različitih tvrtki, koji se redovito obnavlja.

Obzirom na sve izneseno u dokumentu, mogu se izvući sljedeći zaključci:

- Iako tvrtke koje razvijaju *keylogger* programe tvrde da su to legalni programski paketi, većina se takvih programa koristi za krađu korisničkih podataka u političkoj i industrijskoj špijunaži.
- Trenutno *keylogger* programi, zajedno sa tzv *phishing* metodama i metodama socijalnog inženjeringa, predstavljaju jednu od najčešće korištenih metoda *cyber* prijevara.
- Tvrtke koje se bave razvojem sigurnosnih alata bilježe stalan rast broja zlonamjernih programa s funkcionalnošću praćenja unosa znakova preko tipkovnice.
- Izvještaji pokazuju da postoji povećani trend uporabe *rootkit* tehnologija u *keylogger* programima zbog izbjegavanja detekcije.
- Samo posebno oblikovana zaštita može otkriti upotrebu *keylogger* programa u špijunske svrhe.

Unatoč vrlo dobrom prikrivanju i zavaravanju nadgledanih korisnika, keylogger alati imaju i svoje slabosti. Upravo te slabosti korisnici mogu iskoristiti za svoju zaštitu, koja može biti realizirana primjenom standardnih antivirusnih programa ili primjenom proaktivne zaštite. Posljednja, i ne odveć sigurna, protumjera je korištenje virtualne tipkovnice.

7. Reference

[1] Prijetnje *keylogger* alata, http://www.zdnetasia.com/techguide/security/0,39044901,62033096,00.htm , rujan 2004.

[2] O *keylogger alatima*, http://www.viruslist.com/en/analysis?pubid=204791931 , ožujak 2007.

[3] Haxdoor *keylogger*, http://www.f-secure.com/v-descs/haxdoor.shtml , siječanj 2006.