CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Mac OS X malware

CCERT-PUBDOC-2009-10-278

+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

Mac OS X je UNIX sustav kojeg razvija tvrtka Apple, a nasljednik je klasičnih Mac OS operacijskih sustava za Macintosh računala. Iako su od početka njegove distribucije razvijani zloćudni programi kojima je cilj bilo narušavanje sigurnosti sustava, u prošlosti nisu zabilježeni značajniji uspješni napadi. Pritom se misli na programe koji se nanosili određenu štetu sustavu i relativno se široko proširili među Mac korisnicima. Tako je stvoreno uvjerenje o sigurnosti Mac OS X operacijskih sustava do te razine da značajan dio korisnika uopće ne smatra potrebnim koristiti antivirusnu zaštitu. Opravdanost takvih uvjerenja sve češće dolazi u pitanje. U posljednjih nekoliko godina bilježi se značajan porast broja zloćudnih programa za Mac OS X. Kao jedan od ključnih čimbenika koji ovaj sustav čine sve zanimljivijom metom napadačima često se spominje porast njegovog udjela na tržištu operacijskih sustava.

U ovom dokumentu razmotrit će se sigurnost Mac OS X sustava sa stanovišta napadača koji ga pokušavaju ugroziti širenjem zloćudnog koda. Osim spomenutog načina, prijetnje sustavu mogu proizlaziti iz različitih programskih ranjivosti koje napadač može iskoristiti za stjecanje neovlaštenog pristupa sustavu, izmjenu podataka i slično. Pritom se misli na različite napade lažiranja identiteta, otkrivanja i izmjene podataka koji se šalju preko mreže i slično. No takve zlouporabe nisu tema ovog dokumenta.

Bit će prikazani primjeri dvaju poznatih zloćudnih programa za Mac OS X. Razmotrit će se i mogućnosti zaštite, od korištenja sigurnosnih mehanizama sustava do antivirusnih alata. Cilj ovog dokumenta u konačnici je predstaviti i razmotriti razinu te ozbiljnost opasnosti koju zloćudni programi predstavljaju za Mac OS X.

2. Zloćudni programi i sigurnost sustava Mac OS X

Mac OS X je operacijski sustav razvijen prema UNIX modelu, a proizvodi ga i distribuira tvrtka Apple Inc. Oznaka „X“ označuje rimski broj deset, jer je prvi Mac OS X sustav nasljednik posljednje inačice klasičnih Mac OS-ova - Mac OS 9. Ovi sustavi namijenjeni su za uporabu na Macintosh osobnim računalima koje proizvodi ista tvrtka. Prvi Mac OS izašao je 1984. godine, a prvi Mac OS X 2001. Riječ je sustavu Mac OS X Server 1.0. Najnovija inačica OS X-a je Snow Leopard (Mac OS X 10.6), koja je objavljena sredinom 2009. godine.

Slika 1. Radna površina Mac OS X Leopard sustava
Izvor: Wikipedia

Ovu vrstu operacijskih sustava karakterizira naglasak na oblikovanju grafičkog sučelja koje se smatra preferiranim načinom rada u odnosu na rad putem naredbi. Zbog toga su kod prvih inačica postojale ozbiljne zamjerke na nemogućnost rada preko naredbenog retka. Mac OS X može se pokretati na Power PC arhitekturama, a novije inačice sustava (Leopard i Snow Leopard) podržavaju i Intelove procesore. Za razliku od njih, klasični Mac sustavi podržavali su samo za Motorola 68000 procesore, a kasnije inačice i Power PC arhitekture.

Slika 2. Prvo Macintosh naspram suvremenog iMac stolnog računala
Izvor: Wikipedia, Apple.com

2.1. Osobitosti Mac arhitekture

Kao i svaki sustav, Mac OS X posjeduje osobitosti koje ga čine u određenim pogledima naprednijim, a u nekim drugim manje naprednim sustavom u odnosu na druge. U dijelu poglavlja koji slijedi razmotrit će se neke osobitosti arhitekture ovog sustava, s posebnim naglaskom na sigurnosnim mehanizmima i specifičnim ranjivostima

2.1.1. Sigurnosna orijentiranost

Mac OS X posjeduje određena svojstva koja ga čine relativno sigurnim sustavom. Za razliku od Windowsa, OS X korisniku ne dopušta mijenjanje i nadograđivanje OS-a bez prethodne provjere administratorskih ovlasti. To znači da nije dovoljno koristiti samo administratorski korisnički račun za obavljanje kritičnih aktivnosti, već je prije svakog takvog postupka potrebno iznova unijeti administratorsku lozinku kao potvrdu ovlaštenog korištenja sustava. Time se sprječava dobar dio napada zloćudnim programima koji se šire preko web-a i elektroničke pošte. Osim toga, UNIX arhitektura bitno je organiziranija i jednostavnija od Windows arhitekture. Transparentnost dopušta postojanje mnogo manjeg broja neuočenih ranjivosti. Za razliku od starijih inačica Windows sustava na kojima je moguće automatsko pokretanje skriptnog HTML koda u elektroničkim porukama, na Mac sustavima tako nešto nije moguće bez prethodne dozvole korisnika. Velik broj napada na Windows sustave ciljao je upravo na tu ranjivost. Zbog spomenute zaštite, Mac OS-ovima ovakve zlouporabe nisu nikada predstavljale prijetnju.

Kod razvoja Mac OS sustava ne vodi se toliko računa o mogućnostima korištenja s različitim sklopovskim uređajima i različitim tehnologijama. Jedan od bitnih uzroka ranjivosti Windows sustava je usmjerenost njegovog razvoja prema usklađenosti s različitim tehnologijama (HP, Dell) i konkurentnosti. Tako je recimo uvođenje *ActiveX* tehnologije radi konkurentnosti *Java applets* tehnologiji uvelo značajne sigurnosne rizike jer se zbog Windows arhitekture ActiveX programima koji se pokreću u preglednika dodjeljuje vrlo visoka razina ovlasti. Budući da Mac OS ne podređuje sigurnost nekim drugim tržišnim zahtjevima, ovakvi problemi na njemu ne postoje.

2.1.2. Specifične ranjivosti

S porastom tržišnog udjela raste i broj napada na Mac OS X sustave. Načini ugrožavanja sigurnosti često su povezani sa specifičnim ranjivostima određene arhitekture. Kod Mac OS X-a značajnijim rizicima mogu se smatrati sljedeća svojstva:

- ***Bundle* direktoriji** – riječ je o mogućnosti stvaranja direktorija kojem korisnik pristupa kao jednoj datoteci. Primjer korisnosti ovakvih struktura je pohranjivanje višestrukih jezičnih datoteka. Njih govornici različitih jezika mogu jednostavno koristiti preko iste bundle datoteke. Pritom se, prema postavkama, odabire samo odgovarajuća jezična datoteka iz direktorija. Mogućnosti zlouporabe ovakvih struktura uključuju podmetanje zloćudnog koda u skriveni direktorij s „.app“ nastavkom. Znači da se radi o programu koji se pokreće preko *bundle* datoteke, a pravi izvršni kod je neka datoteka u bundle direktoriju. Ta se datoteka u direktoriju može zamijeniti zloćudnim kodom, a da korisnik ništa ne nasluti jer pokreće naizgled isti program.
- **Nezaštićeni „/Applications“ direktorij** – korisnički programi na Mac OS sustavima (iTunes, iChat, Keynote i sl.) spremaju se u navedeni direktorij. Za razliku od programa sustava koji se štite ograničavanjem pristupa, pristup korisničkim programima u direktoriju „/Applications“ potpuno je slobodan. Ako se uzme u obzir mogućnost slobodne izmjene programskih datoteka i bundle arhitektura koja te promjene skriva od korisnika mogućnosti zlouporabe postaju još očitije.
- **Skrivanje vrste datoteka** – Mac OS X dopušta skrivanje pravog nastavka datoteke (npr. „.app“, „.jpg“) čime se omogućuje podmetanje naizgled bezazlenih datoteka koje su zapravo izvršne („.app“) i sadrže zloćudni kod. Ova mogućnost inače postoji i na Windowsima.
- **Nezaštićeni adresar** – na Mac sustavima svi podaci o korisničkim kontaktima (IM adrese, elektronička pošta, brojevi telefona, fizičke adrese i sl.) čuvaju se u jedinstvenoj, nezaštićenoj bazi. Ovakva se ranjivost može iskoristiti primjerice za nekontrolirano širenje računalnih crva.

Slika 3. Bundle datoteka i direktorij
Izvor:MacForensicsLab

2.2. Zloćudni programi za Mac OS X

Zloćudni programi za Mac OS sustave razvijali su se otkad je objavljena prva inačica klasičnog Mac OS-a (inačice do uključivo 9). Njihova brojnost bitno je manja od one brojnosti štetnih programa za Windows sustave. Ipak posljednjih godina zloćudni programi pokazali su se kao rastuća prijetnja Mac OS X sustavima koja zahtjeva pažnju. Kratak uvod u vrste zloćudnih programa, njihove načine djelovanja i korisnička uvjerenja koja im olakšavaju integriranje u sustav dani su u nastavku poglavlja. Detaljniji opisi zloćudnih programa mogu se naći u na službenoj stranici CERT-a pod kategorijom „Crvi i virusi“.

2.2.1. Vrste zloćudnih programa

Tri su osnovne vrste zloćudnih programa:

1. virusi,
2. crvi i
3. trojanski konji.

Virusi su računalni programi koji se umeću u izvršni kod drugog programa te preko njega čine štetu i šire se. Oblikuje ih se na taj način da imaju dvije funkcije:

- prepisivanje vlastitog koda u novi program domaćin – zbog ovakvog načina širenja infekcijom drugog programa dobili su naziv.
- nanošenje štete sustavu – osim širenja često imaju i određenu funkciju koja može biti bezazlena (jednostavna obavijest korisniku da je infekcija uspješna i virus prisutan) ili vrlo destruktivna - brisanje osjetljivih datoteka, rušenje sustava i sl.)

Virusi za svoje djelovanje koriste ovlasti korisnika koji je pokrenuo izvođenje inficiranog koda. Svako pokretanje zaraženog programa pokrenut će i virusni kod.

Crve također karakterizira sposobnost samostalnog širenja. Za razliku od virusa, oni se ne šire uz pomoć programa domaćina, već to čine slanjem vlastitih kopija kroz mrežu. S druge strane, oni u pravilu ne nanose štetu datotekama na sustavu, već samo mreži. Njihov primarni cilj je širenje što može dovesti do zagušenja mrežnih kanala.

Trojanski konji dobili su naziv prema tome što se predstavljaju kao korisni program koji ostvaruju određenu funkcionalnost. Na taj način korisnika se navodi na njihovu instalaciju i pokretanje. U sebi često sadrže:

- određeni koristan kod koji osigurava korištenje i pokretanje trojanskog konja i

- zloćudni kod koji nanosi štetu sustavu.

Šteta primjerice može biti otkrivanje i slanje osjetljivih podataka napadaču. Kod ove vrste napada vrlo je važan faktor korisnička neopreznost koja dovodi do preuzimanja programa i datoteka sa sumnjivih i nepouzdanih mrežnih izvora.

2.2.2. Povijest zloćudnih programa na Mac OS sustavima

Jedan od prvih računalnih virusa - „Elk Cloner“, razvijen je za Apple DOS sustav 1982. godine. Prenosio se preko disketa tako što se prepisivao u memoriju računala na kojem je operacijski sustav podizan s diskete koja sadrži virus. Iz memorije računala se potom prepisivao na nezaražene diskete. Nije činio nikakvu štetu, samo je svaki pedeseti put kod podizanja sustava na zaslonu prikazivao ispis virusne poruke (slika 4).

Slika 4. Ispis Elk Cloner virusa
Izvor: MacForensicsLab

Prvi klasični Mac OS izdan je 1984. godine. Skupa s distribuiranjem sustava počeo je razvoj zloćudnih programa za ovaj sustav. Jedan od poznatijih je „nVir“ iz 1987. Virus se prenosio preko zaraženih programa u koje je umetao svoj kod. Izazivao je rušenje korisničkih programa i programa sustava. Kôd ovog virusa objavljen je javno što je dovelo do razvoja mnogobrojnih njegovih inačica (npr. AIDS, f__k, Hpat, Jude, nVIR, MEV#, MODM, nCAM, nFLU, kOOL i _HIT). Razvoj klasičnih Mac OS-ova redovito je pratio razvoj zloćudnih programa. Neka od važniji poboljšanja koja je Apple tvrtka uvela u Mac sustave kako bi poboljšala njihovu sigurnost je isključivanje mogućnosti automatskog pokretanja programa s umetnutog diska (eng. autorun). Primjerice, Windows sustavi još uvijek koriste ovu tehnologiju što dovodi do mogućnosti pokretanja (i širenja) zloćudnog koda bez dozvole korisnika.

Od objave prvog Mac OS X sustava 2001. pa sve do 2006. godine nije zabilježen niti jedan značajniji napad zloćudnim programima. Prvim se često smatra IM (eng. Instant Messaging) crv naziva „OSX/Leap-A“ čija će se svojstva detaljnije obraditi u zasebnom poglavlju. Od tada do danas broj crva, virusa i trojanskih konja za Mac sustave raste nezanemarivom brzinom. Do 2006. nije bilo poznatih virusa za Mac OS X, a danas ih ima preko 20. Na stranici besplatnog antivirusnog alata za Mac sustav – „iAntiVirus“, može se naći popis poznatih prijetnji za klasične i OS X Mac sustave.

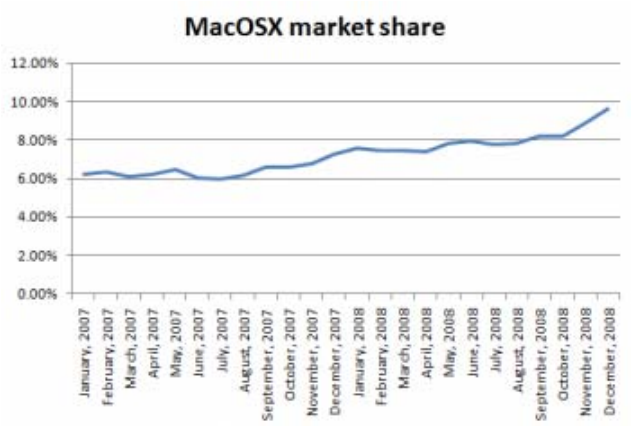
Trojan.OSX.Lamzev.a		Trojan.OSX.Lamzev.a is a Trojan horse that opens a back door on the compromised computer.
Trojan.OSX.RSPlug.A		Trojan.OSX.RSPlug.A is a Trojan horse that modifies the Domain Name System (DNS) settings of the affected system.
Trojan.OSX.RSPlug.B		Trojan.OSX.RSPlug.B is a Trojan horse that modifies the Domain Name System (DNS) settings of the affected system.
Trojan.OSX.RSPlug.C		Trojan.OSX.RSPlug.C is a Trojan horse that modifies the Domain Name System (DNS) settings of the affected system.
Trojan.OSX.RSPlug.D		Trojan.OSX.RSPlug.D is a Trojan horse that changes the DNS settings on the compromised computer.
Trojan.OSX.RSPlug.E		Trojan.OSX.RSPlug.E is a Trojan horse that changes the DNS settings on the compromised computer.
Trojan.OSX.RSPlug.F		Trojan.OSX.RSPlug.F is a Trojan horse that modifies the Domain Name System (DNS) settings of the affected system.
Trojan.OSX.RSPlug.G		Trojan.OSX.RSPlug.G is a Trojan horse that modifies the Domain Name System (DNS) settings of the affected system.
Trojan.OSX.RSPlug.K		Trojan.OSX.RSPlug.K is a Trojan horse that changes the DNS settings on the compromised computer.
Trojan.OSX.RSPlug.M		Trojan.OSX.RSPlug.M is a Trojan horse that changes the DNS settings on the compromised computer.
Trojan.OSX.RSPlug.N		Trojan.OSX.RSPlug.N is a Trojan horse that changes the DNS settings on the compromised computer.
Trojan.OSX.RSPlug.O		Trojan.OSX.RSPlug.O is a Trojan horse that changes the DNS settings on the compromised computer.

Slika 5. Popis prijetnji za Mac OS X
Izvor: iAntiVirus

2.2.3. Načini iskorištavanja ranjivosti sustava

Zloćudni programi na Mac OS X sustavima najčešće se oslanjaju na neopreznosti korisnika i integriraju se u sustav uz pomoć trojanskih konja. Potom se lako mogu prepisati i proširiti u druge dijelove sustava što je posljedica nedostatka posebne zaštite direktorija i datoteka.

Općenito je rašireno uvjerenje da su Mac operacijski sustavi sigurni. Do takvog se zaključka dolazi zbog relativno rijetkih napada na ovaj operacijski sustav zabilježenih u prošlosti. Ipak, rijetkost napada na sigurnost Mac sustava nije isključivo posljedica njegove dobre zaštite već i nedovoljne „zanimljivosti“ njegovih korisnika. Relativno mali udio na tržištu i češće korištenje za osobne potrebe (nego za poslovne) čini Machintosh računala manje zanimljivom metom napadačima. Windowsi do danas zauzimaju gotovo 90% tržišta, a Mac tek počinje prelaziti 10%. Osim toga, s porastom udjela na tržištu počeli su se javljati i prvi napadi na Mac OS X. Zato je pogrešno uzimati sigurnosti Mac sustava „zdravo za gotovo“ samo zato jer u prošlosti nije bila bitno narušavana. Cijeli kontekst govori da je sigurnost nešto o čemu treba voditi sve više računa u cjelokupnom području informacijskih tehnologija, uključujući i ovu vrstu OS-a.



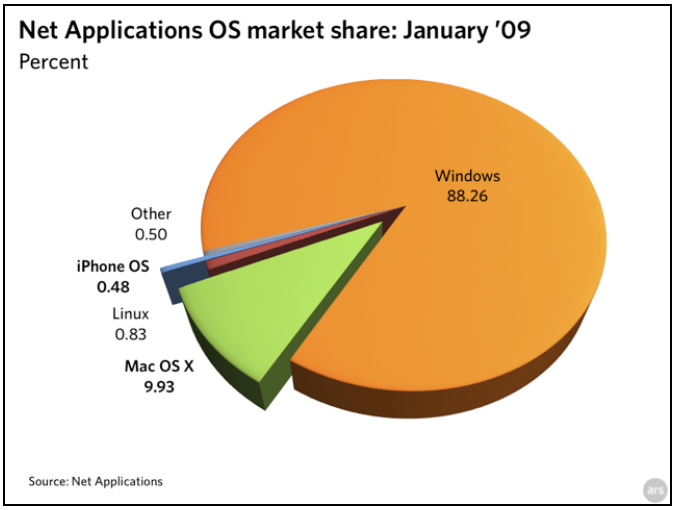
Slika 6. Porast tržišnog udjela Mac OS X sustava
Izvor: SuccessfulSoftware.net

Bez obzira na arhitekturu koja je oblikovana s većim naglaskom na sigurnosti od primjerice Windows sustava, porast prijetnja nije zanemariv. Pogotovo zato što se ranjivosti nalaze koliko u sustavu toliko i u svijesti korisnika koji pod lažnim osjećajem sigurnosti neoprezno preuzimaju različite programe s Interneta i ne koriste dostupne sigurnosne mehanizme.

Činjenica je da računalni sustavi mogu biti dobro zaštićeni, ali jamstva njihove sigurnosti zapravo nema. Dobra obrana može biti narušena dovoljno dobro osmišljenim napadom. Pritom se podrazumijeva pronalaženje i iskorištavanje njezinih ranjivosti. Što je motivacija za

rušenje obrane veća (npr. veća materijalna korist) to je veća vjerojatnost da će se netko potruditi osmisliti dobar napad. U tom smislu budućnost bi mogla otkriti još više Mac ranjivosti s obzirom da porast udjela na tržištu povećava i motivaciju napadača.

Porast tržišnog udjela Mac OS X sustava posljedica je sve atraktivnijih inačica, posebice Leopard i Snow Leopard. One uvode čitav niz poboljšanja kao što su potpora za Intelove procesore, potpuna potpora za programe namijenjene 64-bitnoj arhitekturi, službena UNIX 03 certifikacija, potpora za višeprocesorska računala i ubrzavanje rada, nova grafička prezentacija sustava i slično.



Slika 7. Tržišni udio Mac OS X sustava početkom 2009.
Izvor: arstehnica.com

Općenito, napadi na računalne sustave postaju sve profinjeniji i sve opasniji. To je povezano i s time što se sve više osjetljivih informacija pohranjuje na računalima i prenosi Internetom. Kao što se razni društveni i ekonomski sustavi preslikavaju na računalnu mrežu, to se događa i s drugim negativnim pojavama kao što su kriminal i terorizam. U takvom kontekstu neopravdano je smatrati Mac OS X ikakvom zaštićenom ili nedodirljivom iznimkom.

3. Primjeri zloćudnih programa

U ovom poglavlju ukratko će se analizirati dva zloćudna programa za Mac OS X sustave. Radi se o crvu *OSX.Leap.A* koji se smatra i prvim zloćudnim programom za Mac OS X te trojanskom konju *OSX.Pupper* čija je posljednja pojava zabilježena sredinom ove godine. U analizi ovih programa opisat će se način njihova širenja, šteta koju nanose sustavu te načini na koje ih se može otkriti i ukloniti sa sustava.

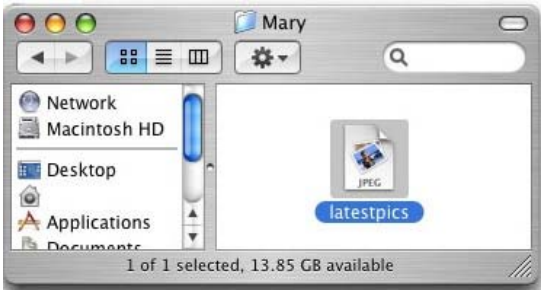
3.1. OSX.Leap.A

Zloćudni program *OSX.Leap.A* je crv koji se pojavio 2006. godine, a smatra se prvim zloćudnim programom za Mac OS X sustave. Ponekad se naziva i virusom zbog sposobnosti da inficira druge programe te se širi pomoću njih. Osim toga ima svojstva trojanskog konja jer se korisnika navodi na njegovo preuzimanje i pokretanje lažnim predstavljanjem. Naime, ovaj crv se korisniku nudi kao JPEG slikovna datoteka. Nije neobično da kod zloćudnih programa postoje rasprave o njihovoj točnoj podvrsti. Ipak po načinu djelovanja, a to je širenje mrežom bez štetnih izmjena u sustavu, ovaj je program najbliže definiciji crva.

OSX.Leap.A djeluje tako da se prenosi preko *iChat* programa, a njegovo pokretanje zahtjeva korisničko preuzimanje i potvrdu. Nakon što se program instalira, sam sebe u maskiranom JPEG obliku šalje drugim korisnicima na popisu liste iChat kontakata inficiranog sustava.

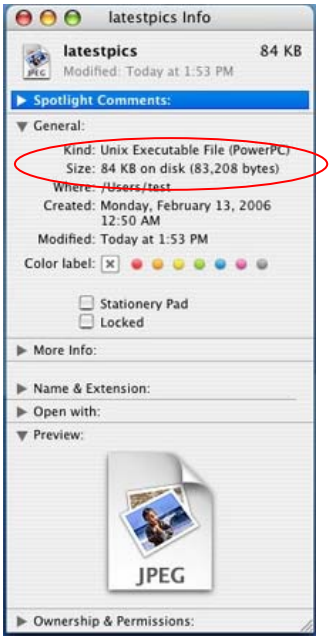
3.1.1. Opis djelovanja

Crv *OSX.Leap.A* korisniku *iChat* programa se nudi kao privitak koji sadrži arhivu s JPEG slikovnom datotekom. Poruka dolazi od korisnika čiji je sustav već inficiran ovim crvom. Izvorna poruka koja je sadržavala ovaj program nudila je navodne slike zaslona Mac OS X Leopard sustava.



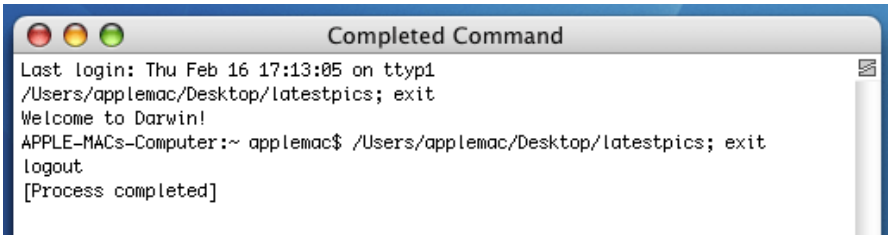
Slika 8. iChat poruka s OSX.Leap.A crvom
Izvor: Viruslist.com

Nakon što korisnik preuzme i otpakira arhivu, može pokušati otvoriti sliku. Budući da je navodna JPEG datoteka zapravo izvršni kod, neće se pojaviti slika već će se pokrenuti program.



Slika 9. Get Info prikaz na kojem se vidi da je datoteka izvršna
Izvor: Viruslist.com

Radi se o programu koji komunicira s korisnikom preko naredbenog retka pa se otvara sučelje prema njemu. Ispisuje se poruka o uspješnom izvođenju procesa. To znači da se crv instalirao na sustav i inficirao programe kojima napadnuti korisnički račun ima pristup.



Slika 10. Ispis naredbenog retka po pokretanju programa
Izvor: Symantec

Zbog pogreške u programskom kodu ovog crva neće biti moguće pokrenuti inficirane programe. Naime, crv kod programa domaćina prepisuje vlastitim kodom, a pritom program domaćina pridjeljuje krivom procesu zbog kojeg ga više nije moguće pokrenuti. Kod pokušaja pokretanja zaraženih programa pokreće se kod crva koji se pokušava slati korisnicima s liste kontakata *iChat* programa.

3.1.2. Tragovi u sustavu

Arhiva koja se šalje preko iChat programa sadrži dvije datoteke: „latestpics“ i skrivenu datoteku „._latestpics” koja se koristi kako bi se lažirao JPEG format *latestpics* datoteke.

Slika 11. JPEG ikona
Izvor: Symantec

Prilikom pokretanja ovog programa stvaraju se sljedeće datoteke:

- /tmp/latestpics,
- /tmp/latestpics.tgz,
- /tmp/latestpics.tar.gz,
- /tmp/hook,
- /tmp/apphook,
- /tmp/pic.gz,
- /tmp/apphook.tar i
- /tmp/pic.

Brišu se svi unosi iz direktorija „~/Library/InputManagers“ i prepisuje se datoteka *apphook* u direktorij „~/Library/InputManagers/apphook/apphook.bundle/Contents/MacOS“. Na taj način osigurava se njezino pokretanje svaki put kad se pokrene neki program trenutnog korisnika. *Apphook* program pokušava širiti zlćudni kod preko *iChat* programa slanjem kopije glavnog tijela crva svim kontaktima.

Nakon toga, crv inficira često korištene lokalne programe koje pronalazi pomoću programa *Spotlight*. Riječ je o alatu koji omogućuje pretraživanje datoteka i direktorija prema zadanim znakovnim nizovima. Pritom inficirane programe označava stvaranjem dodatnog datotečnog atributa „oompa“ i postavljanjem njegove vrijednosti na „loompa“.

Prisutnost crva može se otkriti pretraživanjem navedenih datoteka i direktorija. Osim toga, inficirani lokalni programi zbog spomenutog programskog propusta u crvu neće ispravno raditi što je također koristan pokazatelj o izvedenom napadu. Primjerom ovog zlćudnog programa pokazuje se nepreporučljivost olakog preuzimanja datoteka putem IM (eng. Instant Messaging) klijenata. Isto se može reći i za elektroničku poštu. Također, datoteke preuzete s nepoznatog izvora valja provjeriti jer vizualno sugerirani format ne mora biti pravi format datoteke.

3.2. OSXPuper.A

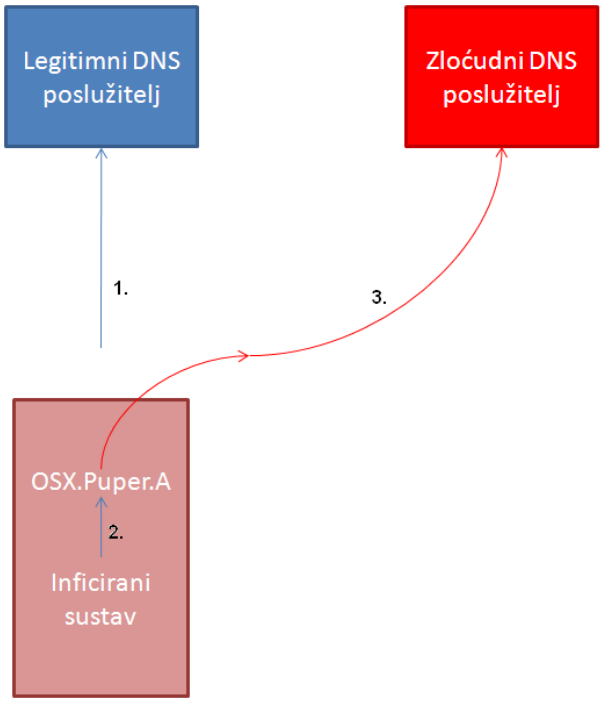
OSXPuper.A je trojanski konj čija se posljednja inačica javila početkom 2009. godine. Prvi put je otkriven još 2007. godine, a osim navedenog naziva poznat je i pod imenom *OSX.RSPlug.A*. Napad se izvodi preko zlćudnih web stranica koje korisnika navode na instalaciju navodnog HDTV (eng. High Definition Television) alata za pregledavanje određenih sadržaja stranice. Ukoliko korisnik nasjedne na prijevaru, preuzet će zlćudni program i instalirati ga na sustav. Prava funkcija ovog trojanskog konja je izmjena DNS (eng. Domain Name System) postavki tako da se korisnika može preusmjeravati na različite zlćudne stranice i izvoditi „phishing” prijevare.

3.2.1. Opis djelovanja

Ovaj program najčešće se širi preko web stranica s pornografskim sadržajem, iako može biti povezan i s bilo kojom drugom vrstom stranica. Prilikom posjeta stranici korisnik se obavještava da na njegovom računalu nedostaje potrebna programska potpora za pregledavanje sadržaja koji je zatražio. Pritom mu se ponudi mogućnost preuzimanja i instalacije potrebnog programa. Ukoliko korisnik potvrdno odgovori, počinje preuzimanje alata. Prije instalacije na Mac OS sustavima najčešće će se zatražiti administratorska lozinka. Ukoliko je neoprezan korisnik upiše program se instalira na sustav.

Nakon instalacije korisnik neće moći pregledati tražene sadržaje jer navodni alat nije instaliran i preglednik će ga automatski vraćati na istu stranicu. Ono što je instalirano na sustavu je program koji mijenja postavke DNS poslužitelja i preusmjerava DNS zahtjeve zlćudnom poslužitelju. To znači da kad korisnik upiše zahtjev za nekom stranicom, npr. www.cert.hr, zlćudni DNS poslužitelj može ga preusmjeriti na IP adresu sasvim druge stranice. Ta stranica može biti stranica sasvim drugačijeg sadržaja, npr. pornografskog ili može biti „phishing“ stranica. Riječ je o zlonamjerno oblikovanim stranicama koje se predstavljaju i izgledaju kao poznate pouzdane stranice (npr. stranica neke banke,

poslužitelja elektroničke pošte ili bilo što drugo). Prijavom korisnika na takvoj lažno predstavljenoj stranici mogu se dobiti osjetljivi podaci kao što su lozinke i korisnička imena.



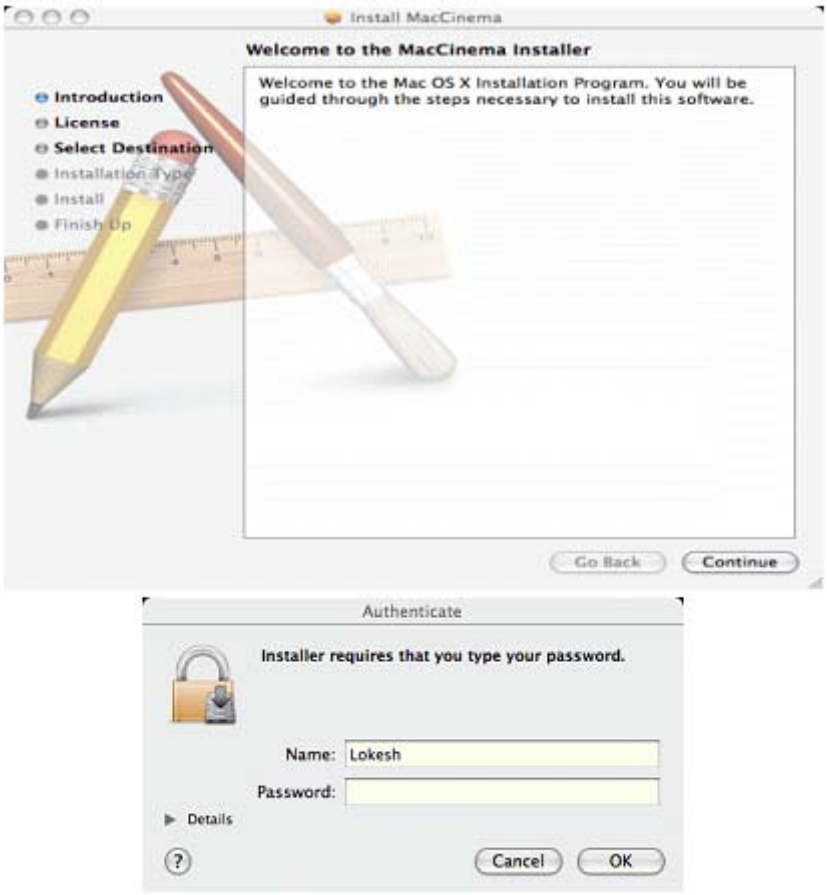
Slika 12. Shema djelovanja zloćudnog programa OSX.Puper.A

Očito je riječ o potencijalno vrlo opasnoj prijevari. S druge strane uloga korisnika u cijelom napadu je ključna jer on sam preuzima kod i odaje administratorsku lozinku. Program nije virus koji se sam instalira i širi izvan dosega korisničkog uvida. Za pristup sustavu traži vrlo visoko povjerenje korisnika. No upravo zbog svoje dobre zamaskiranosti trojanski konji predstavljaju veliki problem u sigurnosti korisnika prilikom korištenja Interneta. Preporučeno ponašanje u ovakvim situacijama bilo bi provjeriti na Internetu informacije o usluzi i alatu koji se želi instalirati na sustav i ukoliko se potreba za njim pokaže stvarnom preuzme sa sigurne i pouzdane stranice (o su najčešće stranice izvornog projekta u okviru kojeg se alat razvija).

3.2.2. Tragovi u sustavu

Nakon što se preuzme i pokrene alat u „.dmg“ formatu, počinje proces instalacije. Ukoliko korisnik odluči nastaviti s instalacijom od njega će se tražiti administratorska lozinka. Pritom se program kopira u direktorij */Library/Receipts*. Osim toga u direktorij */Library/Internet Plug-Ins* pohranjuju se dvije zloćudne skripte „AdobeFlash“ i „Mozillaplug.plugin“. Pritom se mijenjaju postavke DNS poslužitelja tako da se zahtjevi preusmjeravaju nekom od zloćudnih poslužitelja (npr. 85.255.115.58 ili 85.255.112.159). Ova se izmjena može vidjeti u programu Terminal (/Applications -> Utilities) pomoću naredbe *scutil* koja je zapravo sučelje prema konfiguracijskom programu sustava *configd*.

Upisom naredbi „*scutil*“ pa potom „*show State:/Network/Global/DNS*“ dobit će se ispis poznatih DNS polužitelja. Zatim se taj popis može usporediti s popisom u GUI sučelju *Network preferences*. Ukoliko ispis *scutils* naredbe sadrži unose koji nisu u popisu Network preferences sučelja, trojanski konj je vjerojatno instaliran.



Slika 13. Poruke kod instalacije programa
Izvor: McAfee

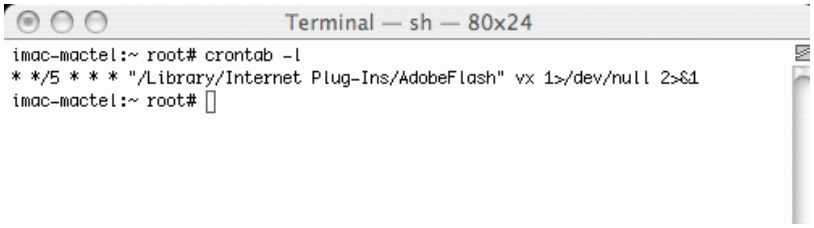
Osim navedenih izmjena, *OSXPuper.a* dodaje zadatak u *crontab* tablicu. Riječ je o mehanizmu kojim se omogućuje automatsko pokretanje pojedinih programa u definiranim vremenskim razmacima. U ovom slučaju zadaje se naredba poput sljedeće:

```
* */5 * * * "/Library/Internet Plug-Ins/AdobeFlash">/dev/null 2>&1
```

Ova naredba osigurava redovito pokretanje zloćudne skripte kako bi se obnovile štetne DNS postavke u slučaju da su u međuvremenu vraćene na pretpostavljene (eng. default) vrijednosti (npr. automatskim postupkom). Postojanje ovakvog *crontab* zadatka može se provjeriti naredbom

```
crontab -l
```

u već spomenutom programu Terminal (slika 14.).



Slika 14. Ispis cron tablice u programu Terminal
Izvor: McAfee

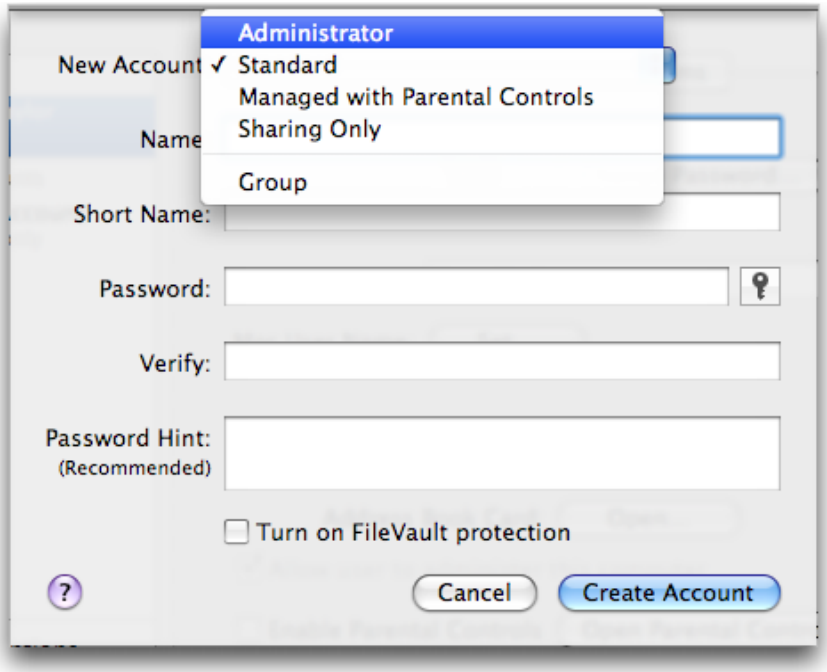
Pretraživanjem navedenih datoteka i postavki sustava moguće je ustanoviti postojanje ovog trojanskog konja na računalu. Otkloniti ga je moguće ručnim brisanjem datoteka te izmjenom DNS konfiguracije i brisanjem automatskog zadatka ili jednostavno korištenjem ažurne inačice nekog antivirusnog alata. Druga navedena mogućnost možda je bolja jer se njome otklanjaju sve poznate prijetnje te nije potrebno svaku ručno obraditi.

4. Zaštita Mac OS X sustava i korisničko ponašanje

Kod analize navedenih dvaju primjera zlođudnih programa uočava se kako se u oba slučaja za uspješnu zlouporabu traži korisnički pristanak. Bez antivirusnih alata praktički je dovoljna korisnička reakcija prije preuzimanja i/ili instalacije datoteke kako bi se napadi spriječili. Mac OS X zaista ima dobre sigurnosne mehanizme i zaštitu pristupa sustavu, ali nije imun na neodgovornost korisnika. S druge strane, s porastom broja prijetnji pitanje je može li se očekivati od korisnika da će prilikom preuzimanja svake datoteke s Interneta i pokušaja njezinog otvaranja poduzeti sve potrebne provjere. Zbog toga ima smisla razmatrati dodatnu zaštitu u obliku antivirusnih programa. U ovom poglavlju dat će se kratki korisnički savjeti za sigurno korištenje Interneta na Mac OS X sustavu i razmotrit će se potreba i smisao korištenja antivirusnih alata.

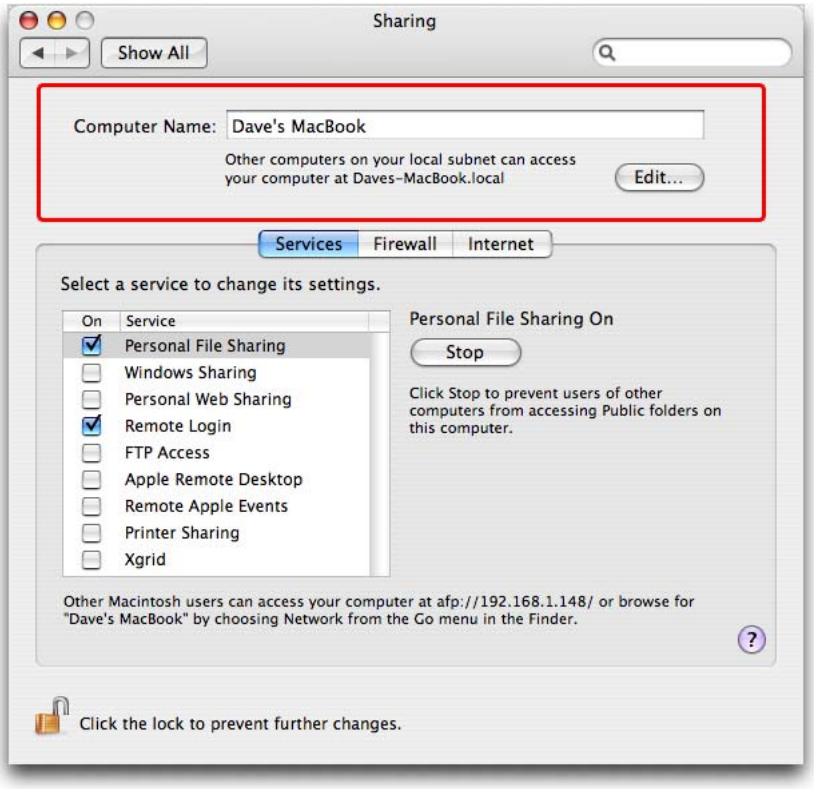
4.1. Korisnički savjeti

Budući da je administratorski račun zbog svojih visokih ovlasti osobito osjetljiv na svim sustavima, ne preporuča se njegovo korištenje u svakodnevne svrhe. Na Mac OS X-u preporučljivo je u „System Preferences" sučelju stvoriti dodatni korisnički račun kojem će se pridijeliti administratorske ovlasti. Potom se s novog administratorskog računa mogu otkloniti administratorske ovlasti izvornog računa koji se redovito koristi.



Slika 15. Stvaranje novog korisničkog računa
Izvor: askdavetaylor.com

Također, korištenje „System Preferences" sučelja osjetljivo je jer se preko njega stvaraju novi računi, mijenjaju mrežne i sigurnosne postavke i sl. Preporuča se uključiti traženje administratorske lozinke kod pristupa bilo kojem od tih sučelja čak i kod korištenja administratorskog računa. Dodatno se u *System Preferences->Sharing* sučelju preporuča isključiti sve usluge koje se ne koriste kako bi se onemogućila njihova nepotrebna zlouporaba.

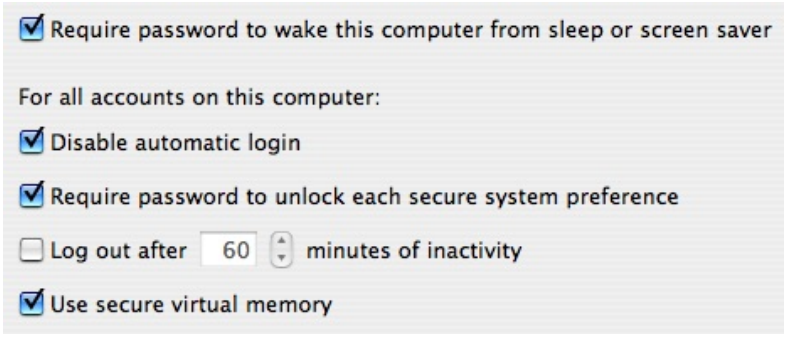


Slika 16. System Preferences -> Sharing sučelje
Izvor: askdavetaylor.com

Iako se širenje zloćudnih programa danas najčešće odvija preko Interneta, ne treba zanemariti i njihovo lokalno podmetanje preko prenosivih memorijskih diskova ili njihovim preuzimanjem preko neovlaštenog lokalnog pristupa. Načini na koje se mogu otežati napadi lokalnih napadača su sljedeći:

- onemogućavanje automatske prijave na sustav otežava zlouporabu napadačima s fizičkim pristupom sustavu,
- traženje lozinke prilikom svakog pokretanja sustava iz stanja priprave (eng. standby) ili odmaranja zaslona (eng. screensaver),
- odjava korisnika nakon nekog zadanog vremena neaktivnosti te
- korištenje sigurne virtualne memorije kako bi se spriječilo otkrivanje prethodno upisanih lozinki – naime ukoliko se ne koristi sigurna virtualna memorija moguće je da se upisane lozinke u nekriptiranom obliku spreme u "/var/vm" direktorij gdje ih napadač može otkriti. Korištenje sigurne virtualne memorije to sprječava jer se datoteke u osjetljivom direktoriju kriptiraju.

Praćenjem ovih naputaka smanjuje se vjerojatnost da će napadač u trenutku korisnikove odsutnosti uspješno podmetnuti zloćudan kod na sustav.

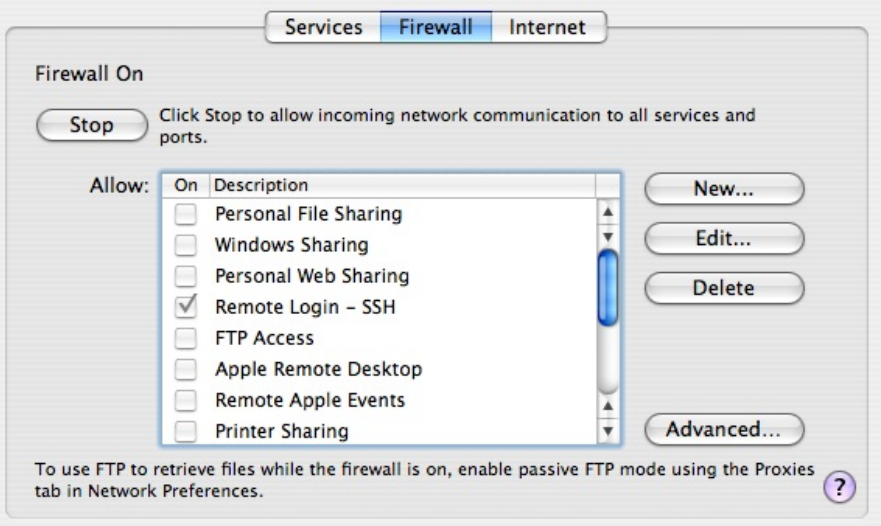


Slika 17. Sigurnosne postavke
Izvor: Mac Geekery

Osim toga, Mac OS X nudi posebnu uslugu za upravljanje lozinkama – *Keychain,* koja se može koristiti za automatsko upisivanje korisničkih lozinki. Naime, kod pristupa pojedinim uslugama potrebno je više puta unijeti različite zaštitne lozinke i ključeve. U slučaju da ovaj alat koristi ovlašteni korisnik, on mu olakšava upotrebu tako što korisnik ne treba upisivati traženu lozinku za svaki korak pristupa. No u slučaju neovlaštenog pristupa napadaču se omogućuje stjecanje pristupa svim alatima i uslugama napadnutog korisničkog računa koji koristi *Keychain* uslugu. Zaključavanjem *Keychain* sustava nakon što računalo prijeđe u stanje priprave osigurava se traženje *Keychain* lozinke nakon njegovog pobuđivanja. Bez te lozinke neće biti moguće pristupiti primjerice IM programima zaštićenim lozinkom. Postavljanjem *Keychain* lozinke na različitu vrijednost od one koja se koristi prilikom prijave na sustav stječe se veća razina sigurnosti na uštrb jednostavnosti korištenja.

Slika 18. Keychain postavke
Izvor: Mac Geekery

Kako bi se onemogućilo djelovanje trojanskih konja koji otvaraju određene TCP priključke preko kojih napadač može pristupati sustavu preporuča se korištenje Mac OS X vatrozida. Njime će se onemogućiti neovlaštena komunikacija preko TCP priključaka.

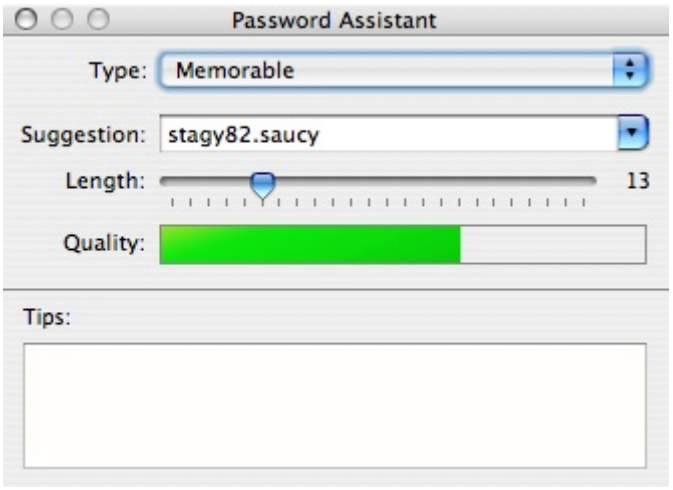


Slika 19. Postavke Mac OS X vatrozida

Izvor: Mac Geekery

Uz to je dobro kod udaljenog SSH pristupa onemogućiti administratorsku prijavu dodavanjem „*PermitRootLogin no*“ retka u „/etc/sshd_config“ datoteku.

Budući da se dobar dio zaštite Mac OS X sustava zasniva na korištenju lozinki, preporučljivo je odabrati sigurne nizove znakova za njihove vrijednosti. To su nizovi bez jezičnog smisla koji se sastoje od slova, brojeva i posebnih znakova kao što su primjerice znakovi interpunkcije. U tome može pomoći alat Password Assistant.



Slika 20. Password Assistant sučelje

Izvor: Mac Geekery

Osim toga, spominjane su ranjivosti arhitekture vezane uz *bundle* strukture te uz mogućnost sakrivanja pravih datotečnih nastavaka. Ova svojstva datoteka mogu se provjeriti na sljedeće načine:

- korištenjem „Get Info“ mogućnosti kod datoteka kako je prikazano na slici 8. u prethodnom poglavlju – dobivaju se informacije o vrsti datoteke.
- provjerom postojanja "Show Package Contents" mogućnosti u izborniku datoteke utvrđuje se je li riječ o bundle strukturi, a izborom te mogućnosti može se pregledati njezin sadržaj.

Slika 21. Primjer sadržaja bundle paketa
Izvor: MacRumors:Guides

4.2. Antivirusni alati

Osim sigurnog korištenja sustava i opreznog korisničkog ponašanja rizik od zloćudih programa moguće je umanjiti korištenjem antivirusnih alata. Za Mac OS X tu su dostupni neka besplatna rješenja:

- ClamXav – riječ je o alatu koji se temelji na ClamAV antivirusnom rješenju. Ne odlikuje ga osobito širok spektar djelovanja, no s obzirom na to da Mac OS X još uvijek nije izložen tako velikom broju zloćudnih programa, ovaj alat može biti sasvim prihvatljivo rješenje.
- iAntivirus – je alat koji je orijentiran isključivo na zloćudne programe za Mac OS X operacijske sustave. Pritom ne podržava zaštitu protiv virusa koji su oblikovani za Windows sustave (neškodljivi Mac OS X sustavima). Zato ovaj antivirus nije najbolje rješenje ukoliko se koristi dvojno okruženje s Mac OS X i Windows sustavima.

Neka od komercijalnih antivirusnih rješenja uključuju:

- Norton Antivirus – uključuje široki spektar zaštite protiv Windows i Mac zloćudnih programa. Neke od dostupnih inačica ove antivirusne zaštite su:
  - Norton AntiVirus Dual Protection – sustav koji nudi dvostruku antivirusnu zaštitu koji koriste Windows i Mac OS X sustave istovremeno ili pokreću Windows virtualno računalo na Macintosh računalu s Intel procesorom.
  - Norton Internet Security 3.0 – je komercijalno rješenje za starije Mac OS X sustave namijenjeno isključivo Power PC arhitekturama.
- McAfee VirusScan – riječ je o alatu koji je podržan na inačicama Mac OS X Tiger i novijim, a može se izvoditi na Intelovim i Power PC procesorima. Također, alat se može koristiti samostalno ili integriran s ePolicy Orchestrator (ePO) paketom za upravljanje poslovnim sustavima.
- Intego VirusBarrier X5 – riječ je o jednom od najskupljih antivirusnih rješenja za Mac OS X sustave (50 do 400 dolara), no ujedno o jednom i od najboljih. Ovaj sustav pruža zaštitu protiv Windows i Mac orijentiranih zloćudnih programa, a može se koristi i na način da se uključi zaštita protiv samo jedne vrste, npr. samo od zloćudnog koda za Windowse. Odlikuje ga i učinkovito te inovativno korisničko sučelje.

Slika 22. Intego VirusBarrier X5 korisničko sučelje
Izvor: Intego

Kod korištenja antivirusnih alata na Mac OS X sustavima često se postavlja pitanje jesu li oni uopće potrebni? Pogotovo zbog toga što je velika većina prijetnji i zlođudnih programa za ovaj sustav oblikovana tako da teško može ući u sustav bez pomoći korisnika. S druge strane, u prošlosti su se više puta pojavile situacije kad su sami antivirusni alati uveli veće ranjivosti u sustav nego što su bile opasnosti od postojećih zlođudnih programa. Svaki programski proizvod može sadržavati sigurnosne propuste. Zbog visokih ovlasti pod kojima rade, ranjivosti antivirusnih alata posebno su opasne.

U svakom slučaju, korisnik prema vlastitim potrebama određuje razinu i vrstu zaštite potrebnu njegovom sustavu. No kad se govori o zaštiti od zlođudnih programa, kvalitetni i odgovarajući antivirusni alat svakako je rješenje koje valja razmotriti.

5. Zaključak

U ovom dokumentu pokušalo se dati uvid u specifične ranjivosti i obrane operacijskih sustava Mac OS X od zlođudnih programa. Budući da su prijetnje programskim virusima, crvima ili trojanskim konjima još uvijek takve da ne uspijevaju naći pristup sustavu bez eksplicitne pomoći korisnika ne mogu se smatrati opasnostima najviše razine. S druge strane, zaštita i korisničko odgovorno ponašanje zahtijevalo bi izvođenje provjera prilikom svakog preuzimanja i pokretanja pojedine datoteke (što se od prosječnog korisnika teško može očekivati). Jednom kada se zlođudni program integrira u sustav, šteta koju može napraviti postaje stvarna i izuzetno ozbiljna. Dodatnu opasnost pritom predstavlja slaba zaštita pojedinih programskih i podatkovnih sadržaja u Mac OS X sustavu.

Prilikom zaštite od štetnih programa jednaku pažnju valja voditi o mrežnoj sigurnosti koliko i o lokanoj i fizičkoj zaštiti računala, osobito ako se radi o prijenosnim uređajima. Konačno, korisnik se može osloniti i na dostupne antivirusne alate koji otkrivaju i otklanjaju štetni kod iz sustava. Veća razina zaštite pritom uvodi veće komplikacije kod korištenja, od čestog unošenja lozinki i potrebe za prijavama i odjavama za različite korisničke račune do usporavanja rada računala zbog antivirusnog alata. Zato je zadatak svakog korisnika da procjeni prioritete i odluči se za optimalnu razinu sigurnosti i učinkovitosti prema svojim potrebama.

Jedna zamka u koju ne bi bilo dobro upasti je uvjerenje o sigurnosti i nedodirljivosti Mac OS X-a samo zato što do sada nisu zabilježeni ozbiljniji napadi. Brojnost zlođudnih programa za ove sustave raste zamjetno brzo. Može se očekivati da će budućnost i sve više zainteresirana populacija napadača ubrzo pronaći ranjivosti i ovog OS-a. Zato potreba za prikladnom zaštitom postaje sve stvarnija i nešto što ne treba nikada maknuti s uma.

6. Reference

[1] Carl Howe, The Mac OS X Malware Myth Continues, http://seekingalpha.com/article/52722-the-mac-os-x-malware-myth-continues, listopad 2009.

[2] Marko Kostyrko, Malware on Mac OS X, http://www.macforensicslab.com/Malware_on_Mac_OS_X.pdf, listopad 2009.

[3] Mary Landesman, Mac Antivirus Software Reviews: The Best and Worst of Mac Antivirus Software, http://antivirus.about.com/od/antivirussoftwarereviews/tp/aamacvir.htm, listopad 2009.

[4] Basic Mac OS X SecurityBasic Mac OS X Security, http://www.macgeekery.com/tips/security/basic_mac_os_x_security, listopad 2009.

[5] OSX/Puper.a, http://vil.nai.com/vil/content/v_154438.htm, listopad 2009.

[6] OSX/Leap.a, http://vil.nai.com/vil/content/v_138578.htm, listopad 2009.