Доц. др Кристијан Кук*
Криминалистичко-полицијска академија, Београд

UDK – 004.738.5 : 004.491.22
Примљено: 20.01.2015.

Рањивост оперативних система на злонамерне програме

Апстракт: *Иако постоји велики број ствари од којих је потребна заштита, главне су оне које се појављују са Интернета. Много штетних програма се инсталира неприметно на рачунар корисника и на њихову инсталацију без одговарајуће заштите не може да се утиче. Кад се то догоди, обично је касно и потребна је детаљна провера целог рачунара. Многи вируси и бројни хакери на мобилним уређајима постају данас све већи проблем у заштити личних информација. Вируси за мобилне телефоне одавно нису новост, већина корисника ових уређаја заражених малвером не зна за инфекцију зато што не знају за безбедносне пропусте њихових оперативних система. У овом раду приказан је преглед одговарајућих оперативних система који подржавају шифровање у односу на изабрани мобилни телефон, што може довести до већег ниво безбедности самог уређаја. Постоји много различитих врста штетних софтвера који утичу на безбедност мобилних уређаја али и на персоналне (личне) рачунарске системе корисника, као што су: вируси, тројанци, малвери, bootkit-ови и други. Master boot сектор, први сектор хард диска у рачунарском систему на коме се налази код потребан за покретање оперативног система, често је мета напада специфичне врсте вируса, тзв. bootkit-ова или rootkit-ова. Пошто су невидљиви за оперативни систем, веома их је тешко уклонити са зараженог рачунара, па се у раду, кроз преглед рањивости оперативних система, скреће пажња на њихов могући напад.*

Кључне речи: *оперативни систем, рањивост, малициозни софтвер, boot сектор вируси*.

* E-mail: kukkristijan@gmail.com

Увод

У свом досадашњем развоју информационо-комуникационе технологије су донеле огромне промене у развоју друштва. Интернет, мобилни телефони и друга савремена средства комуникације постали су неизбежни део савременог друштва. Живот се у последњој деценији XX века изменио захваљујући и изузетном технолошком напретку. Технологија је постала моћан алат, међутим она може бити и злоупотребљена јер је уједно постала и глобално доступна, па самим тим расте и број потенцијалних ризика од напада са Интернета. Интернет је увећао лакоћу и брзину којом се спроводе противправне активности, уклањајући физичка ограничења и смањујући физички напор за превару (Krutz, Vines, 2001: 11). У данашње време информација је један од најважнијих и најскупљих ресурса у пословању. Њено правовремено поседовање, њена исправност и тајност често су од одлучујуће важности у пословању било које институције.

Потребно је истаћи да чак и најспремније (по питању безбедности) организације могу бити суочене са противправним активностима, као што су дела преваре, крађе, упада у рачунарске системе, финансијске преваре, крађа интелектуалне својине (Ћикановић, 2010: 139), DDOS напади (Čisar, 2013: 113), подметање малициозних програма и друге противправне активности. На пример, инциденти који се дешавају у оквиру организације углавном се односе на проблем као што је ширење малициозних програма (на пример вируса, црва, шпијунских програма).

Малициозни софтвер или скраћено малвер (*malware*) је софтвер који је дизајниран да се инфилтрира у компјутерски систем без информисања и пристанка његовог власника. Ово је општи термин који користе стручњаци да опишу различите облике непријатељског, наметљивог или досадног софтвера или програмског кода. Израз „компјутерски вирус“ обухвата све типове малициозног софтвера, као и праве вирусе.

Вируси, црви и тројански коњи су злонамерни програми који могу да изазову штету на рачунару и подацима који су на њему. Они такође могу да успоре Интернет везу, па чак и да користе корисников рачунар за даље ширење на рачунаре корисникових пријатеља, породице, колега, као и на остатак веба. Малициозни код на инфицираном рачунару може да: изврши брисање/преузимање осетљивих фајлова, прави од корисника извор заразе на Интернету, прати све покрете на тастатури, може да гребује видео садржај са камера на корисничком компјутеру или аудио сигнал са микрофона, да маскира своје присуство скривајући фајлове, процесе и употребу мреже (Sikorski, Honig, 2012: 5).

Оперативни системи

Модерни компјутерски системи се састоје од једног или више процесора, меморије, дискова, тастатуре, дисплеја и других улазно-излазних уређаја, што представља сложен систем. Писање програма који надзиру ове компоненте и правилно их користе је врло тежак посао. Из тог разлога компјутери поседују „слој“ софтвера, назван оперативни систем (скраћено ОС), чији је посао да управља свим овим уређајима и да обезбеди корисничке програме који имају једноставне интерфејсе према хардверу.

При томе хардвер рачунара представља „сирову“ рачунарску моћ, а задатак оперативног система је да хардверске могућности учини доступним и по могућности удобним за сваког корисника (Silberschatz, Galvin, Gagne, 2004: 31). Дизајн и израда оперативног система је уско повезана са хардвером као основом на којој се оперативни систем изграђује, па зато произвођачи хардвера најчешће производе и своје оперативне системе. Због тога имамо више различитих приступа, нивоа, верзија и намена оперативних система (Tanenbaum, 2012: 33). Корисник види оперативни систем преко језика за кумуникацију са њим (командни језик, контролно-управљачки језик), а већина унутрашњих проблема, решења и поступака оперативног система за корисника је транспарентна (он о њима не мора да води рачуна, нити их мора познавати).

Уз управљање рачунарским ресурсима − процесорима, оперативном меморијом, периферним уређајима и подацима, оперативни системи треба да обезбеде интерпретирање и извођење контролно-управљачких команди и програма, управљање пословима, заштиту, а често и подршку даљинске обраде и рада у мрежи.

Корисник комуницира са оперативним системом преко контролно-управљачког (командног) језика. Комуникација се одвија у два смера: од корисника ка оперативном систему и обрнуто. Код већине савремених оперативних система корисник може да оперативном систему задаје команде непосредно и посредно. Непосредно задавање команди подразумева да оперативни систем одмах по уношењу командне линије врши њену анализу и интерпретацију. Посредно задавање команди подразумева да се низ-пакет (*batch*) захтева оперативном систему забележи у фајл, а да се тај фајл касније по потреби позива на извршење навођењем његовог имена. Инструкције командног језика, било да су задате непосредно једна по једна или у пакету, обрађује командни интерпретер.

Учитавање оперативног система

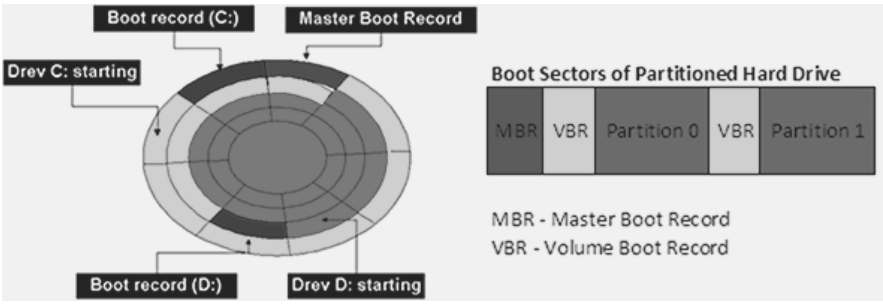
Оперативни систем док рачунар ради мора бити учитан у радну меморију рачунара. Кад је рачунар искључен, радна меморија је празна. Бутовање (*booting*) представља процесс иницијализације рачунара и покретања оперативног система. Бутовање се састоји од следеће три фазе:

1. покретање *BIOS*-а;
2. извршавање *bootloader*-а;
3. покретање оперативног система.

BIOS (*Basic Input/Output System*) представља први софтвер који се покреће приликом покретања рачунара. Задужен је за иницијализацију, проверу и управљање периферним уређајима, а пре свега оним са којих се може покренути оперативни систем. *BIOS* има само могућност провере (*Power-on self test*). *BIOS* је задужен за налажење уређаја који је погодан за подизање система и извршавање *bootloader*-а са његовог *boot* сектора. *Bootloader* је програм задужен за покретање оперативног система. Ако се ради о диску, требало би да се налази на његовом првом сектору (*MBR − Master Boot Record*).

Слика 1 − *Процес покретања оперативног система*
(Извор: https://eugene.kaspersky.com/2013/08/01/protection-against-bootkits, доступно 15.02.2014.)

У првих 512 *byte*-а хард диска уписани су подаци о томе како је диск подељен на партиције и која је партиција диска системска. Системска партиција мора бити означена као активна (ознака − заставица 'A'). Наведени блок података назива се *MBR* и ако се записи оштете, губе се сви подаци. *MBR* је независан од оперативног система, а садржи запис о начину на који је диск (или више њих) подељен на партиције и која је од њих активна (Smith, 2010: 119). При томе, две партиције не могу бити истовремено активне.



Слика 2 – *Boot сектори на партиционисаном хард диску*
(Извор: http://www.howtoretrievefiles.com/about-data-recovery/logical-failure, доступно 15.02.2014.)

MBR запис је прво што се очита од стране иницијалног програма (*bootstrap*) записаног у *BIOS*-у који када пронађе бут ознаку активне партиције, очитава *boot* сектор, сектор активне партиције диска у којем је запис о томе где се налази датотека под називом *boot_manager*. Ова датотека (која је обично на адреси C:\bootmgr) користи *BCD* записе (*Boot Configuration Data*) у фолдеру (који је обично на адреси C:\boot) како би сазнао више о оперативном систему који мора покренути, или да понуди неки избор ако се користи више оперативних система. Приликом учитавања верзије *Windows 7* оперативни систем даљи надзор препушта датотеци под називом *windows loader*, тј. *winload.exe* или датотеци *windows resume loader*, односно *winresume.exe*, који је обично на адреси C:\Windows\System32 или C:\Windows\System32\boot. Датотека *winload.exe* алоцира радну меморију и учитава неопходне системске управљачке програме и даљи надзор препушта језгру оперативног система – кернел *ntoskrnl.exe*. Ова датотека, величине неколико MB, обједињује фундаменталне делове оперативног система и смештена је у фолдеру C:\Windows\System32. У случају оштећења система датотека или враћања из стања хибернације користи се датотека *winresume.exe*. Након тога, активира се датотека *smss.exe* (*Session Manager Subsystem*) у фолдеру на адреси C:\Windows\System32, где се учитавају варијабле окружења и врши приступ виртуелној меморији, након чега следи пријава корисника на систем преко програма *winlogon.exe*.

Дакле, редослед акција приликом укључивања рачунара би био следећи: BIOS, POST, BootStrap > MBR > Boot Sector > Boot Manager > WINLOAD.EXE > NTOSKRNL.EXE > SMSS.EXE > WINLOGON.EXE.

Сервиси на оперативном систему

Једна од најбитнијих ствари које чине оперативни систем су његови сервиси. Сервиси су врста процеса који покрећу разне компо-

ненте, програме, скриптове у рачунарском систему. Сервиси на рачунару су мањи програми који раде у позадини. То су програми који омогућавају функционисање рачунарске мреже, *USB* флеш дискова, других компонената рачунара и, у суштини, цео оперативни систем функционише помоћу њих. Већину процеса треба оставити да раде и не треба их заустављати јер би се тада нарушио нормалан ток извршења операција.

Посматрано у окружењу *Windows*-а, сервис представља извршну датотеку која је покренута на релативно дуг период и извршава одређене функције, дизајниране тако да не захтевају интервенције корисника. У зависности од подешавања сервиси могу бити активни у меморији све док је рачунар укључен или их други програми могу покретати по потреби (Ранђеловић, 2009: 286).

ИП адреса је идентификациони број рачунара, односно уређаја у мрежи, а порт је број (од 0 до 65535) прикључка на рачунару на којима се одвија нека мрежна апликација и може бити отворен или затворен (Ranđelović, 2012: 19).

Злонамерни програми – вируси

Злонамерни програмски кодови (малвери) су програми чији је задатак да се убаце или оштете рачунар без знања његовог корисника. Програми се сматрају злонамерним узимајући у обзир намеру нападача, а не особине самог програма. Злонамерни програмски кодови укључују вирусе, црве, тројанце, *rootkit*-ове, *spyware* и друге злонамерне и непожељне програме.

На почетку рачунарског доба злонамерни програми су писани као експерименти или шале које су више сметале кориснику него што су чиниле озбиљну штету на рачунару. Млади програмери писали су злонамерне програме како би видели колико је далеко догурало њихово знање. Међутим, даљим развојем рачунарске технологије појављује се све више оваквих примера. Појавом Интернета циљ нападача је постао профит, незаконито оглашавање и криминал.

Вирус

Вирус је програм или програмски код који се закачи на програм или датотеку тако да може да се преноси са рачунара на рачунар, ширећи при томе заразу. Вируси могу да оштете софтвер, датотеке на рачунару, као и сам хардвер рачунара. Вирус је код написан са јасном наменом да сам себе умножава. Једном када се рачунар зарази вирусом, он се може копирати и изменити самог себе како би теже био откривен. Најчешће се убацују у извршне датотеке програма (*executables*) и при

покретању заражене датотеке шире се на друге. Међу рачунарским вирусима постоје они који су само мала сметња при раду, али и они који су потпуно деструктивни.

Данас се за описивање деструктивног софтвера чешће користи израз злонамеран или малициозан софтвер, тј. малвер. Охрабрујућа чињеница је да се прави вирус не шири без људских поступака који би га покретали, као што су дељење датотеке или слање е-поруке. Вирус се обично састоји од два дела. Први део је самокопирајући код, који омогућава размножавање вируса, а други део је корисни терет (*payload*) који може бити безопасан (бенигни) или опасан (деструктиван, малигни). Неки се вируси састоје искључиво од самокопирајућег кода и немају никакав корисни терет (Szor, 2005: 64).

Врсте рачунарских вируса:

- *boot* сектор вируси − нападају *master boot* сектор;
- паразитски − заразе извршне датотеке додавањем свог садржаја у структуру програма;
- свестрани вируси (multipartite) − нападају *boot* секторе и извршне програме;
- вируси пратиоци (companion) − стварају .com датотеку користећи име већ постојећег .exe програма и уграђују у њу свој код;
- линк вируси − у трену инфицирају нападнути рачунарски систем, могу изазвати велику штету на хард диску;
- макро вируси − имају могућност да сами себе копирају, бришу и мењају документе.

Ова подела првенствено води рачуна о начину на који вирус може заразити различите делове рачунарског система. Без обзира којој групи припада, сваки вирусни код мора бити извршен да би прорадио и размножавао се. Основна разлика између различитих вируса је у начину на који то покушавају да изведу.

Boot сектор вируси

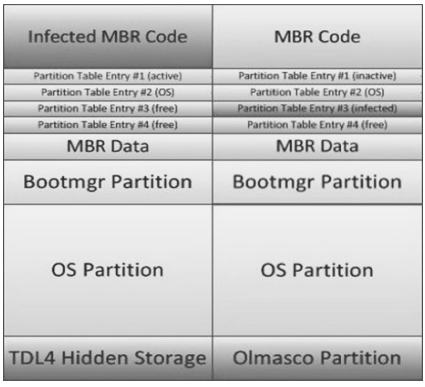
Boot сектор вируси нападају *master boot* сектор, односно његову партициону табелу (*partititon table*), тј. програм који се у њима налази. *Boot* сектор је идеалан објект за инфекцију, будући да садржи први програм који се извршава на рачунару, чији се садржај може мењати. Када једном рачунар буде укључен, програм *BIOS* који се налази у *ROM* меморији ће без питања учитати садржај *master boot* сектора у меморију и извршити га. Ако се у њему налази вирус, он ће постати активан (Florio, Kasslin, 2008: 6). *Boot* сектор вируси се могу ширити и помоћу посебних програма, тројанских коња, званих бацачи (*dropper*), којима је

главна намена да неприметно „убаце“ вирус у *boot* сектор. *Boot* сектор вируси су веома успешни у размножавању – од седам најчешћих рачунарских вируса чак шест их је способно да зарази *boot* сектор.

Нулти сектор хард диска је *master boot* сектор, на коме се налази код потребан за покретање оперативног система након што *BIOS* изврши почетне провере. Због тога се овакви малициозни програми чији се код уписује у *MBR* често називају *bootkit* или *rootkit*, јер се учитавају на тако ниском нивоу, током *boot* процеса, пре покретања оперативног система и антивирусног софтвера. Због тога што су невидљиви за оперативни систем веома их је тешко уклонити са зараженог рачунара.

Управо је то разлог због којег аутори малвера све чешће као мету бирају *MBR*. Са малициозним кодом, какав је и *Popureb*, бојно поље остаје изван оперативног система а свака безбедносна противмера антивирусног софтвера примењена унутар оперативног система може бити избегнута.

Инфекције *MBR* су на неко време потпуно ишчезле након што се завршила ера ДОС вируса (Giuliani, 2011). Онда се крајем 2007. године појавио *Mebroot*, први малвер који је погодио MBR после дужег одсуства *MBR* инфектора. У међувремену, *bootkit*-ови или *rootkit*-ови су значајно напредовали, па смо се тако претходних година сусретали са напредним *rootkit*-овима као што су *TDL4* или *Whistler bootkit*, све до малициозних програма из групе *ransomware*, који врше енкрипцију оригиналног MBR кода и потом заражене компјутере претварају у таоце док њихови аутори или криминалне банде које стоје иза оваквих малвера од корисника компјутера не добију новац којим они откупљују кључеве за декодирање.



Слика 3 – *Хард диск заражен TDL4 bootkit вирусом*
(Извор: http://www.welivesecurity.com/2012/01/03/bootkit-threat-evolution-in-2011-2, доступно 15.02.2014.)

Напади на оперативни систем

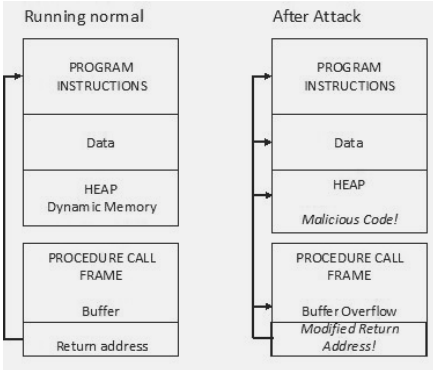
Упад на систем подразумева добијање приступа кроз коришћење рањивости система, као и добијање привилегија на систему. Злонамерно добијање приступа на систему најчешће се остварује на два начина: нападом на оперативни систем и нападом на програме инсталиране на систему.

Када је реч о нападу на оперативни систем, сервиси и отворени портови представљају главне слабости које су предмет искоришћавања. Што је више сервиса и отворених портова, то је више приступних тачака на систему. На основу оваквог гледишта, подразумевана инсталација оперативног система треба да буде са што мањим бројем покренутих сервиса (само неопходним) и отворених портова (уколико је потребан већи број, могу се накнадно инсталирати сервиси). Међутим, у реалности то није случај. Подразумевана инсталација садржи велики број покренутих сервиса и отворених портова, а разлози за инсталирање великог броја сервиса при подразумеваној инсталацији оперативног система која са собом носи огроман безбедносни ризик јесу материјални. Циљ произвођача је да корисник оперативног система може да инсталира и конфигурише систем са најмање напора. То значи да, с једне стране, имамо смањење трошкова за произвођача, а с друге стране имамо већу функционалност на систему и веће задовољство корисника приликом инсталације система (при чему се инсталира и оно што је потребно и оно што није). Са становишта произвођача то је прихватљиво, али са становишта безбедности није. Додатни проблем лежи у чињеници да корисници рачунарских система нису довољно свесни рањивости система које користе. Исто тако, у многим организацијама сматрају да је инсталирањем оперативног система на рачунару посао завршен и не примењују крпљење и ажурирање система (*update*) које се препоручује на дневном нивоу (Sinchak, 2004: 161).

При сагледавању напада на програме инсталиране на систему узроке треба тражити у њиховом развоју јер безбедност није имплементирана у дизајн самог програма. У пракси се програмери који развијају програме сусрећу са врло кратким роковима датим за њихову реализацију. То значи да се тестирање не извршава детаљно. Такође, додатни проблеми који се тиче безбедности настају приликом повећавања функционалности и комплексности програма, па су шансе за тестирање свих функција још мање. Злоупотреба функционалности отвара врата за компромитовање безбедности на систему. На пример, један *e-mail* клијент може да садржи функцију која омогућује директно ишчитавање *html* поруке за корисника. Нападач ово може да искористи тако што осмисли лажну поруку која у *html* изгледа регуларно, али

садржи хиперлинк који води до злонамерне веб странице када корисник кликне на њу (Scarfone, Mell, 2009: 1). Други проблем који се односи на програме јесте испитивање на грешке (*error-checking*). Један од разлога великог броја безбедносних пропуста у програмима је управо недостатак испитивања грешака. *Buffer overflow* је један од примера овог проблема, и ту рањивост може злоупотребити нападач да добије приступ систему, привилегије, а може и да онемогући сервисе на систему. Прекорачење бафера може да изазове крах или неправилно извршење програма, а најчешћа последица је рањивост кôда коју нападачи могу искористити (Плескоњић, 2007: 505).

Напад типа *buffer overflow* настаје када нападач покушава да ускладишти већи број података у бафер меморију у односу на број који је програмер предвидео, проузрокујући тако преливање података са малициозним кодом у друге бафере. Пример за препуњавање бафера може се илустровати на следећи начин: програм очекује низ од 80 знакова, а корисник унесе 300. Када се изврши овај код, нападач може да добије потпуну контролу над системом (One, 1996: 12). Постоје два типа препуњавања бафера: стек и гомила. Стек и гомила представљају две области у меморијској структури које се додељују приликом покретања програма. Позиви функција се чувају у стек области, а динамичке променљиве се чувају у области гомиле. Злонамерни нападачи могу да користе *buffer overflow* гомилу са циљем да измене шифру, име фајла или друге податке. Уколико се име фајла измени, други фајл ће бити отворен. То значи да ће уколико је то нека извршна датотека, бити извршен код који није требало да се покрене.



Слика 4 – *Тип напада buffer overflow*
(Извор: http://cis1.towson.edu/~cssecinj/modules/cs2/buffer-overflow-cs2-java, доступно 15.02.2014.)

Безбедност оперативних система на мобилним уређајима

Са аспекта безбедности постоје различити напади на комуникациони канал мобилног телефона, односно на радно окружење мобилног уређаја. Претње по безбедност мобилног уређаја класификоване су по својој припадности, а делимо их на четири класе: хардверске, типске независне, софтверске и корисничке (Muthumanickam, Ilavarasan, 2014: 2383-2384).

Хардверски напади припадају делу безбедности мобилних уређаја са аспекта ширег становишта. Ове врсте напада се извршавају преправком већ уграђеног хардвера. Пошто захтевају физички приступ хардверу мобилног уређаја, овакви напади нису лаки за злоупотребу, тј. не могу бити даљински искоришћени.

У *типски независне* нападе спадају прислушкивање етра преко *WiFi* мреже и цурење података кроз произвођачево инсталирање неауторизованих сервиса који омогућују „задња врата“ (*back door)*. Нападач уз помоћ одговарајуће опреме прислушкује комуникациони канал између два корисника, детектује појединачне слабости, убацује се у канал и враћа некоректне податке. У случају напада на могући *back door* нападач има неометану могућност модификовања, односно нарушавања интегритета података. Овакви напади не зависе од типа или врсте уређаја.

Софтверских напада има више врста. Догађају се извршавањем малициозних програма или крађом идентитета мобилног претплатника (шпијунажа). Ови напади најчешће могу бити финансијски мотивисани. Напади се могу извршити и преко одређених сервиса мобилне телефоније као што су *SMS, MMS, EMS, GPRS*, преко мобилног Интернет претраживача, кориснички инсталираног злонамерног софтвера, као и антивирусног система за заштиту.

Кориснички оријентисани напади користе слабости које нису техничке природе. Многи малициозни програми за мобилне уређаје користе сигурносне пропусте који нису техничке, односно програмске природе, а својим покретањем извршавају низ корисничких неовлаштених процеса. Захваљујући својој природи заобилазе сигурносне механизме, чиме повећавају ниво рањивости оперативног система.

Поред оперативних система, као што су *Windovs Mobile* и *Simbian OS*, мобилни свет је током последњих неколико година забежио и појаву *iPhone iOS* и *Linux Android* оперативног система. Иако су у питању младе технологије, оба оперативна система су већ стекла велики удео на тржишту мобилних уређаја, а у будућности се очекује њихов још већи раст. Табела 1 даје преглед глобалне продаје на тржишту оперативних система за мобилне уређаје.

Табела 1 − *Преглед употребе оперативних система за мобилне уређаје, март 2011.* (www.gartner.com)

Оперативни систем	**2009.**	**2010.**	**2011.**	**2012.**
Android	3,9%	22,7%	38,5%	48,8%
BlackBerry	19,9%	16%	13,4%	11,1%
iOS	14,4%	15,7%	19,4%	17,2%
Symbian	46,9%	37,6%	19,2%	0,1%
Windows Mobile	8,7%	4,2%	5,6%	19,5%
Остали	6,1%	3,8%	3,9%	3,3%
Укупна продаја у милионима	172	297	468	631

Избором мобилног телефона са одговарајућим оперативним системом који подржава шифровање постиже се већи ниво безбедности. Потребно је изабрати мобилни телефон чији оперативни систем подржава хардверски базирано шифровање. Оперативни систем *iOS* фирме *Apple* и *BlackBarry Research In* подржавају шифровање на интерне и екстерне меморије. Ако уређај нема могућност шифровања, могуће је да неко поврати податке на уређају чак и без корисникове блокаде пина или лозинке. Код *Android* оперативног система пуно шифровање је ограничено на произвођача уређаја. Верзије *Android* 2.3 већ нуде могућност шифровања података, док се од верзије 3 нуди подршка за рад са *API* функцијама које нуде шифровање и на таблет уређајима. *Android* би од верзије 4 требало да подржи шифровање у мобилним телефонима.

Када мобилни корисник користи јавно доступну *WiFi* мрежу преко одређене приступне тачке која не нуди услугу шифровања, повећава се могућност пресретања и модификовања поруке која се преноси кроз етар (Веиновић, Чалић, Бркић, 2012: 92). Најзначајније локације које пружају услуге, као што су сајтови банака, обично имплементирају своју сопствену конекцију *https/ssl* која штити њихов индивидуални мрежни саобраћај. Већина социјалних мрежа не подржава овај безбедносни интерфејс, тако да постоји могућност манипулације подацима који се чувају у мобилном уређају. С друге стране, ћелијски оријентисане мреже (као што су *3G* и *4G*) омогућавају шифровање од стране мобилног оператера тако да прислушкивање на овим типовима веза није толико популарно.

Закључак

Злонамерни софтвер, односно штетни програм, је софтвер који покушава да украде податке са рачунара, пошаље нежељену пошту или почини превару. Ова врста софтвера обично без знања корисника долази уз бесплатне преузете садржаје са Интернета. Корисник није ни свестан да се на некој веб локацији којој приступа налази злонамерни софтвер који се шири на кориснике који приступају тој локацији. То је тако јер је злонамерни софтвер могуће добити приликом преузимања додатака за веб локацију или кода који се инсталира за различите апликације. Уобичајени симптоми злонамерног софтвера су: нежељена преусмеравања *url*-ова, искакајући огласи, измењени *Google* резултати претраге, додатне нежељене траке алата или бочне траке за претраживање у веб прегледачу и успорена брзина рада рачунара.

Ако се нова трака алата одједном појави на web прегледачу или ако су претраживања траке алата преусмерена на други претраживач, постоји велика могућност да рачунар има инсталиран злонамерни софтвер. Злонамерни софтвер некада се преузима са бесплатним преузимањима без знања корисника. Када је инсталиран, може покретати искакајуће огласе, преусмеравати корисника на нежељене веб локације, па чак и изменити изглед и функционалност услуге *Google* претраживање веба на рачунару корисника. Злонамерни софтвер ни на који начин није повезан са траком алата и помоћу њега не може се никакав софтвер инсталирати. Ако на рачунару не постоји неки антивирус програм, први знак да је рачунар заражен је његово успорење. Споро ради, споро се гаси или му кад се упали, треба времена да подигне систем. Такође, ако у доњем десном углу, код сата, почну да искачу обавештења као што су: *Scan your PC, Your PC infected...* итд., то је знак да је рачунар корисника покупио вирус са Интернета или неког *usb* флеш диска. Најчешће се преко друштвене мреже Фејсбук „запати“ тројански коњ, кликом на неки видео снимак који захтева инсталацију додатног програма за преглед. Посетом сајтовима са порнографским садржајем на рачунару се неприметно могу инсталирати штетни малвер програми и програми који памте сваки притиснути тастер на тастатури (*keyloger*). Употреба старије верзије *Internet Explorer*-а као подразумеваног веб претраживача може да зарази компјутер. *Internet Explorer* је иначе слабо отпоран на разне нападе са Интернета. Посећивање сајтова који нуде „*crack, kaygen, patch*“ углавном проузрокује преузимање и тројанског коња, малвера или вируса. Зато је врло опасно скидати и, још горе, инсталирати било какав крек. Крековани програми углавном садрже вирусе.

Уз толико злонамерних програма и вируса који утичу на рачунаре и мобилне уређаје, важно је бити упућен на опасност која вреба. Ако корисник није пажљив, може да се нађе у озбиљној невољи.

Према наводима америчке агенције која се бави безбедносним пропустима, *National Vulnerability Database (NVD*), у 2014. години је у просеку свакодневно регистровано 19 нових рањивости. Што се тиче безбедности, велико је изненађење да *Microsoft Windows* више није на првом месту када је у питању број пријављених безбедносних пропуста. На првом месту је *Apple Mac OS X* са укупно пријављених 147 рањивости прошле године, од којих су 64 класификоване као претње на високом нивоу. На другом месту је такође *Apple*, тачније његов мобилни оперативни систем *iOS*. У 2014. је за *Apple iOS* укупно пријављено 127 рањивсти, од којих су 32 класификоване као претње на високом нивоу. На високом трећем месту налази се *Linux* са 119 пријављених рањивости, од којих су 24 класификоване као претње на високом нивоу.

Литература

1. Čisar, P., (2013). System for detection of intrusions into information infrastructure, *NBP – Journal of Criminalistics and Law*, Vol. 18, No. 1, pp. 113-128.
2. Ђикановић, П., Мојсиловић, Ж., (2010). Примена СМАРТ картица као идентификационих докумената, *Безбедност*, Vol. 52, бр. 3, pp. 139-157.
3. Florio, E., Kasslin, K., (2008). *Your computer is now stoned (... again!)*, Virus Bulletin.
4. Giuliani, M., (2011). *Removing Popureb Doesn't Require a Windows Reinstall*, weblog: Webroot, http://www.webroot.com/blog/2011/06/30/removing-popureb-doesnt-require-a-windows-reinstall, доступно 30. 6. 2011.
5. Krutz, R. L., Vines, R. D., Stroz, E. M., (2001). *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, Chichester.
6. Muthumanickam, K., Ilavarasan, E., (2014). *Demanding Requirement of Security for Wireless Mobile Devices: A Survey*, Research Journal of Applied Sciences, Engineering and Technology 8(24): pp. 2381-2387.
7. One, A., (1996). *Smashing the Stack for Fun and Profit, Phrack*, Vol. 7, Iss. 49.
8. Плескоњић, Д., Мачек, Н., Ђорђевић, Б., Царић, М., (2007). *Сигурност рачунарских система и мрежа*, Микро књига, Београд.

9. Ранђеловић, Д., Петровић, Л., Ранђеловић, Р., Поповић, Б., (2009). EnCase форензички алат, *Безбедност*, Vol. 51, бр. 1-2, pp. 286-312.
10. Ranđelović, D., Stojković, D., (2012). Possibilities of autopsy tool use for forensic purposes, *NBP – Journal of Criminalistics and Law*, Vol. 17, No. 3, pp. 19-33.
11. Scarfone, K., Mell, P., (2009). *The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities (DRAFT), NIST Interagency Report 7502 (Second Public Draft), Computer Security Division Information Technology Laboratory*, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930.
12. Shinder, D. L., (2002). *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress Publishing, Inc., pp. 512.
13. Sikorski, M., Honig, A., (2012). *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*, San Francisco, CA 94103.
14. Silberschatz, A., Galvin, P. B., Gagne, G., (2004). *Operating Systems Concepts.7th Edn*., John Wiley & Sons.
15. Sinchak, S., (2004). *Hacking Windows XP*, Wiley Publishing, Inc., Indianapolis, Indiana.
16. Smith, W. R., (2000). *The Multi-Boot Configuration Handbook. Que Publishing*, Indianapolis, Indiana, pp.260–261.
17. Szor, P., (2005). *The Art of Computer Virus Research and Defense, Addison Wesley*, Pearson Education, Symantec Press.
18. Tanenbaum, S. A., (2012). *Modern Operating System*; 3rd Edn., Prentice Hall, Learning Private Limited, USA.
19. Веиновић, М., Ћајић, М., Бркић, Б., (2012). *Технике и методе напада на комуникациони канал при преносу података у мобилној телефонији*, 10. Међународни научни скуп „Синергија 2012“, pp. 89-94.

The Vulnerability of Operating Systems to Malicious Programs

Abstract: *Although there are many things that need protection, the main ones are those that appear on the Internet. Many harmful programs instal themselves surreptitiously on the user's computer and their infiltration cannot be influenced without proper protection. When this happens, it is usually too late and a thorough inspection of the whole computer is needed. Many viruses and hackers on many mobile devices are becoming an increasing problem in today's protection of personal information. Viruses for mobile phones have been known for a long time, yet the majority of users of these*

devices infected with malware are not aware of the infection because they do not know for the existence of security vulnerabilities of their operating systems. This paper presents an overview of the corresponding operating systems that support encryption in relation to the selected mobile phone, which can lead to a greater level of security of the device. There are many different types of harmful software that affect the security of mobile devices as well as personal computer systems of users, such as viruses, Trojans, malware, bootkits and others. Master boot sector, the first sector of the hard disk in a computer system which contains the code needed to run the operating system is often the target of specific types of viruses called bootkits or rootkits. Since they are invisible to the operating system it is very difficult to remove them from an infected computer. Therefore the review of the existence of vulnerabilities in operating systems offered in this paper is an attempt at drawing attention to their possible attacks.

Keywords: operating systems, vulnerability, malicious program, *boot* sector viruses.