Srednja šola Slovenska Bistrica
Ulica dr. Jožeta Pučnika 21
2310 Slovenska Bistrica

Seminarska naloga pri predmetu
POSLOVNA INFORMATIKA

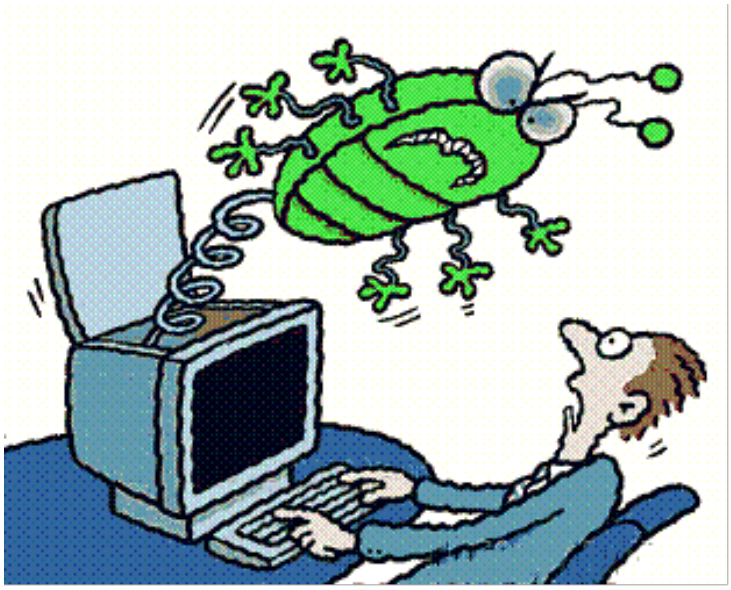
RAČUNALNIŠKI VIRUSI

Slovenska Bistrica, 24. 10. 2009

1 UVOD

V današnjem času viruse zasledimo vse povsod, pojavljajo se v računalnikih, mobitelih, USB ključih, ter v vseh ostalih napravah, ker je to možno. Virusi so samo eden od različnih

tipov programov, ki so narejeni z zlobnimi nameni. Pogosto imenujemo viruse tudi računalniške črve, trojanske konje in ostale vrste zlobnih programov. To lahko zmede uporabnike, saj so dandanes virusi veliko manj pogosti, kot so bili včasih. Danes prevladujejo predvsem trojanski konji in črvi. Zaradi tega se uporabniki pogosto varujejo samo pred določenim tipom zlobnih računalniških aplikacij in so bolj ranljivi za ostale.
Virusi so uničevalci datotek na našem računalniku. Uničujejo razne datoteke, kot se je zgodilo eni osebi na banki ko so ji uničili bančni račun in ni mogla na banki dvignit svojega denarja. Prav tako se ti lahko zaradi raznih virusov zruši cel računalnik in ostaneš brez vseh datotek., kot se je to zgodilo meni, saj sem dobila na računalnik viruse in se mi je kasneje zrušil cel računalnik in sem zaradi tega ostala brez datotek, varnostne kopije pa prav tako nisem imela. Pred virusi se lahko zaščitimo z raznimi protivirusnimi programi in smo tudi previdni pri uporabi interneta, ker na internetu najdemo največ virusov.



Slika 1: Računalnik in virusi[1]

2 KAJ SO RAČUNALNIŠKI VIRUSI

2.1 Virusi

Računalniški virusi so programi , ki se sami razmnožujejo in prenašajo med računalniki. Prenašajo se lahko na fizičnih medijih (CD-jih, disketah …) ali preko omrežij. Virusi se

[1] Vir: dostopno na naslovu: http://files.gsobar.uni.cc/GRADIVA_informatika_omrezja_baze/colos/informatika/INFORMATIKA/RACUNALNISKA_OMREZJA/virusi_crvi_files/image002.gif

ne morejo prenašati sami, temveč rabijo računalnik v katerem se lahko naselijo. Namen virusov je povzročiti škodo, zato moramo vedno imeti posodobljen anti-virusni program, ki nas opomni na prisotnost virusa. Samo ime "virus" izhaja iz dejstva, da je virus potem, ko je okužil magnetni medij, težko odkriti, saj lahko preteče nekaj časa od okužbe pa do trenutka,ko virus začne povzročati težave (virusi, ki se zaženejo na določen datum). Do nedavnega so se virusi prenašali v glavnem preko disket (piratske kopije programov, igrice, preizkusni programi).Računalniški virus je računalniški program, ki se je sposoben sam razširjati preko drugih računalniških programov ali dokumentov. Zaradi tega se računalniški virus obnaša zelo podobno biološkemu virusu, ki se širi tako, da okuži celice. Podobno kot se *okužimo* z biološkim virusom, se tudi računalniški program okuži z virusom. Pogosto potem rečemo, da je računalnik dobil virus. Računalniški program je v tem primeru gostitelj virusa. Čeprav je lahko namen virusov, da uničujejo podatke, so pogosto samo nadležni. Nekateri virusi se sprožijo šele po tem, ko mine določen čas od prvotne okužbe računalnika, ob določenih časih ali ko okužijo zadostno število drugih računalnikov. Večina virusov je kljub temu usmerjena v lastno nekontrolirano reprodukcijo, kar troši računalniška sredstva, kot so procesorska moč, pomnilnik ali količina prostega trdega diska.

Slika 2: Virusi[2]

2.2 Vrste virusov

Viruse lahko razdelimo v tri osnovne skupine:

- Programski virusi: postanejo aktivni ob zagonu določenega programa.
- Virusi zagonskega sektorja: postanejo aktivni ob vklopu računalnika, ko se izvršijo določene procedure, ki se odčitajo z diska.

[2] Vir: dostopno na naslovu: http://cathylwood.files.wordpress.com/2009/04/computer-virus-bugs-clip-art-thumb3167674.jpg

- Makro virusi: postanejo aktivni ob odprtju okuženega dokumenta.

2.3 Virusi bolj podrobno

-Bootstrap Sektor viruses - so virusi, ki okužijo sektor, ki služi za začetno nalaganje. Virus spremeni glavni zagonski sektor (odvisno od vrste virusa in od tipa diska). Virus zamenja obstoječo (legitimno) vsebino s svojo vsebino, originalna verzija zapisa pa se zapiše nekje drugje na disk, tako, da se ob zagonu računalnika vedno prvi aktivira virus, šele nato zagonska procedura. Virus je aktiven, dokler se računalnik ne izključi. Posledica delovanja virusa je občutnejše počasnejše delovanje računalnika.
- Parasitic viruses - zajedalski virusi, ki okužijo "exe" in "com" datoteke. Virus postane aktiven ob zagonu programov. Deluje tako, da spremeni osnovno kodo v programu, kar povzroči nepravilno delovanje programov.
- Multi - partite viruses - večnamenski virus ima lastnosti virusov, ki okužijo sektor za začetno nalaganje in zajedalskih virusov. Virus postane aktiven ob zagonu računalnika in ob zagonu programov (exe, com).
- Companion viruses - okužijo predvsem "exe" datoteke in kreirajo sami "com" datoteke, ki imajo isti naziv kot je "exe" datoteka. Virus postane aktiven ob zagonu "com" datotek.

Slika 3: Računalniški virus[3]

2.4 Kako se virusi širijo

Veliko virusov se širi s pomočjo elektronske pošte, kjer je virus pripet k sporočilu tako, da uporabnik pošte ne vidi. Če od neznane osebe prejmete elektronsko pošto s prilogo, jo takoj zbrišite. Žal niste več varni niti pri odpiranju prilog, ki vam jih pošljejo znanci. Virusi znajo namreč krasti podatke iz programov za elektronsko pošto in pošljejo svoje kopije na vse naslove, ki jih imate v adresarju. Če dobite elektronsko pošto s sporočilom, ki ga ne razumete ali ga niste pričakovali, vedno povprašajte pošiljatelja in se prepričajte o vsebini priloge, preden jo odprete. Drugi virusi se lahko širijo s programi, ki jih prenesete z interneta ali z okuženimi disketami,CD-ji in USB ključi, ki si jih sposodite od prijateljev.

[3] Vir: dostopno na naslovu:
http://beta.financeon.net/pics/cache_F_/F_1_racunalniski_virus_SHU.1201513002.jpg

3 ZGODOVINA VIRUSOV

3.1 Zgodovina virusov

Leta 1984 je bila prvič omenjena možnost računalniških virusov. Takrat je ni nihče jemal resno. Ko pa se je leta 1986 pojavil prvi virus imenovan brain, je bila to prava senzacija. To senzacijo bi lahko imenovali kar genialnost, seveda če se sklicujemo na besede znanega ameriškega ekonomista Galbraitha, ki je nekoč dejal, da ni genialnost izdelati nov izdelek, ki ga trg potrebuje, ampak ustvariti potrebo po izdelku, ki ga ljudje sploh ne potrebujejo. In računalniških virusov zagotovo nihče ne potrebuje.
Prvi virus brain se je najprej razširil v ZDA in ni imel škodljivih efektov. Le malokdo je takrat v virusih videl veliko nevarnost za podatke v računalniških sistemih. Prvi virusi so bili namreč povečini neškodljivi (izpisovali so npr. le kakšno sporočilo na zaslonu), pozneje pa se je začelo pojavljati vse več virusov, ki uničijo ali spremenijo podatke.
Oktobra 1993 je bilo tako znanih že več kot 3000 različnih virusov. Vendar se število teh virusov več ne povečuje tako hitro, kot se je še do leta 1992. Vodilni protivirusni centri v svetu tako zdaj dobijo v analizo okoli 100 novih virusov na mesec. Poleg samega števila sespreminjajo in stalno izboljšujejo tudi tehnike skrivanja in načini razmnoževanja virusov.

4 VIRUSI PROBLEM SODOBNE DRUŽBE

4.1 Znaki okužbe z virusom

Najpogostejši znaki z okužbo z virusom so:

- izguba podatkov na magnetnem mediju,
- samodejno delovanje tiskalnika
- izvršilne datoteke (EXE, COM) spremenijo velikost
- neprekinjena obdelava podatkov na trdem disku
- samodejno izvajanje ukazov v uporabljenem programu
- zvočni efekti
- operacijski sistem se ne naloži,
- pospešeno delovanje računalnika

Slika 4: Virusi veliki problem[4]

4.2 Antivirusni programi

Antivirusni programi so programi, ki varujejo računalnik pred virusi. Lahko jih uporabljamo samo za direktno preverjanje posameznih datotek, lahko pa so v stalni pripravljenosti in sproti preverjajo datoteke, s katerimi delamo ali pregleduje elektronsko pošto.

Ko antivirusni program zazna virus, lahko:

- okuženo datoteko očisti,
- okuženo datoteko izbriše (izguba podatkov),
- datoteko postavi v osamitev (karanteno), kjer je širjenje virusa onemogočeno.

Antivirusni programi ponavadi omogočajo naslednje zaščite:

Anti-Virus: zaščita pred virusi, trojanskimi konji, črvi (vključno z zaščito e-pošte)

[4] Vir: dostopno na naslovu: http://varujem.com/slike/trojanec.jpg

Anti-Spyware: zaščita pred programčki, ki nepooblaščeno zbirajo informacije
Anti-Rootkit: zaščita pred programčki, ki lahko prevzamejo nadzor nad računalnikom
Anti-Spam: zaščita pred neželjeno elektronsko pošto
WebShield: zaščita pred zlonamernimi spletnimi stranmi
Firewall: požarni zid, zaščita pred vdori v računalnik

Nekaj glavnih antivirusnih programov:

- Symantec Norton antivirus
- NOD 32
- Norman
- AV

Slika 5: Anty-Virus System[5]

4.3 Trojanski konj

Trojanski konj je posebni tip računalniškega virusa, ki ga nepridipravi uporabljajo za dostop ali pregled računalnikov v podjetju z oddaljene lokacije in s strani tretje (nepooblaščene) osebe. Trojanskega konja lahko uporabijo tudi zato, da namestijo nove programe na vaše računalnike brez vašega vedenja, pošiljajo elektronsko pošto ali pregledujejo vašo internetno povezavo in podatke, ki jih vpisujete na spletna mesta (gesla, uporabniška imena, naslov itd).

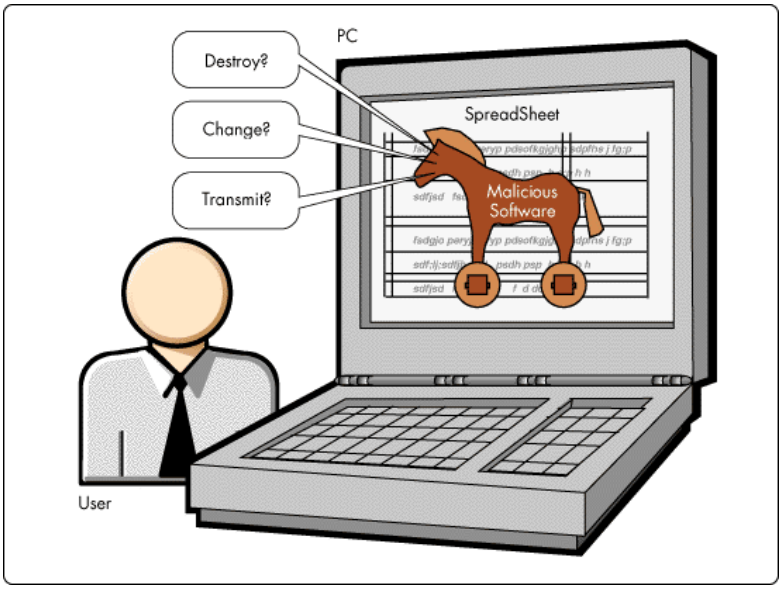
[5] Vir:pridobljeno na naslovu: http://www.bdtutors.com/marketplace%20images

Trojanski konj se pogosto širi z odpiranjem okuženih priponk v elektronski pošti, obiskom okuženih spletnih mest ali z odpiranjem programov, ki jim zaupamo in jih dnevno uporabljamo (Microsoft Windows, Microsoft Office, itd).

Z upoštevanjem pravil varne uporabe interneta boste svoje računalnike tudi zavarovali.

Svetujemo vam, da sledite naslednjim korakom:

- Uporabljajte posodobljeno protivirusno zaščito.
- Ne odpirajte elektronske pošte od neznanih oseb.
- Ne odpirajte priponk, ki ste jih prejeli po elektronski pošte, če ne veste, kakšen je njihov namen.
- Vedno uporabljajte zadnjo različico operacijskega sistema z vsemi dostopnimi varnostnimi popravki.
- Gesel in uporabniških imen ne zapisujte v elektronska sporočila ali v dokumente, ki jih hranite na računalniku.



Slika 6: Trojanski konj[6]

4.4 Računalniški črv

Računalniški črv je prav tako kot virus, ki se širi iz računalnika v računalnik, vendar tako, da sam izvaja funkcije računalnika za prenos datotek ali podatkov. Ko se črv naseli v sistem, lahko potuje sam. Velika nevarnost črvov je njihova sposobnost izjemno hitrega širjenja. Pojavil se je črv Mydoom, ki se je pojavil februarja 2004, je uporabil posebej nadležen način prepričevanja uporabnika, da klikne priloženo datoteko. Njegov avtor je natančno izdelal več navidezno legitimnih sporočil o napaki z naslovi "Mail Delivery

[6] Vir:pridobljeno na naslovu: http://support.novell.com/techcenter/articles/img/ana1997110106.gif

System," "Test" ali "Mail Transaction Failed". Te vrste elektronske pošte najbrž prejemate redno. To so uradna sporočila, ki nas obveščajo, da eno od naših poslanih e-poštnih sporočil ni doseglo naslovnika. Pogosto vsebujejo tehnično besedilo, ki ga večina ljudi ne razume. Avtor črva Mydoom je ta jezik posnemal in tako prepričal milijone uporabnikov, da so odprli prilogo.

Poznejše različice črva Mydoom so uporabile taktiko strahu, saj bila e-poštna sporočila takšna, kot bi jih poslal prejemnikov ponudnik internetnih storitev. Sprejemnika so opozarjala, da je okužen s črvom in da je tega mogoče iz računalnika odstraniti edino z odprtjem priloge. Kot ste morda že ugotovili, so prav te priloge vsebovale črva.

Širjenje črva: Eden od nadležnih načinov širjenja črvov je pošiljanje e-poštnih sporočil s škodljivimi prilogami na vse naslove v uporabnikovem adresarju. Tako se črv zakrije kot e-pošta prijatelja, ki mu zaupamo. Zato je izjemno pomembno, da smo pazljivi pri odpiranju e-poštnih prilog.

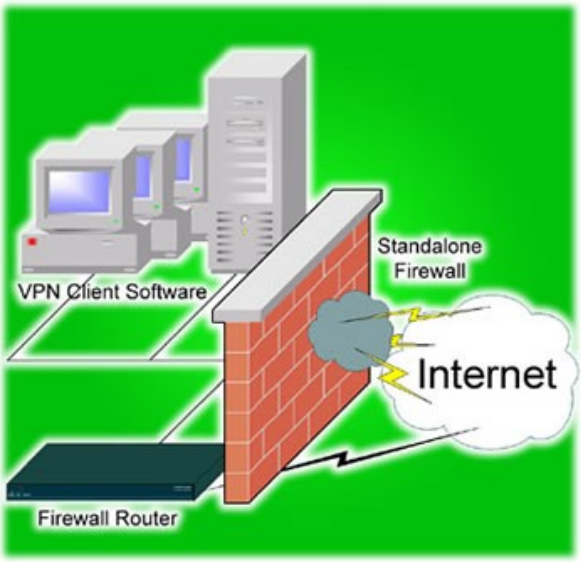
Slika 7: Širjenje računalniških črvov[7]

4.5 Požarni zid

Požarni zidovi so postali nepogrešljiv del,zaščite pred nevarnostmi, ki prežijo na internetu. Po nekaterih raziskavah računalnik, ki je v internet povezan neposredno, brez varnostnih popravkov operacijskega sistema, brez protivirusnega programa in brez požarnega zidu, 'preživi' le štiri minute. Požarne zidove v grobem delimo na strojne in programske. Tiste, ki so del strojne opreme, uporabljajo predvsem podjetja, saj so takšne

[7] Vir:pridobljeno na naslovu: http://www.microsoft.com/slovenija/doma/varnost/virusi/zivljenjski_cikel_crva.mspx

naprave precej drage, njihova prednost pa je predvsem hitrost. Domače računalnike največkrat ščitijo programski
požarni zidovi. Microsoft požarni zid v svoje operacijske sisteme vključuje vse od varnostnega paketa popravkov SP2 za Windows XP. Ena od največjih pomanjkljivosti njihovega požarnega zidu pa je ta, da preverja le vhodni promet, ne pa tudi izhodnega. Velik del programov, ki jih imamo nameščene na računalniku, komunicira preko interneta bodisi z ali brez naše vednosti. Programi največkrat na strežnikih, s katerimi komunicirajo, iščejo posodobitve ali javljajo statistiko, požarni zid pa mora biti sposoben takšne komunikacije pravilno oceniti in v primeru, da gre za neželeno komunikacijo, ukrepati. Od požarnih zidov pa ne moremo pričakovati, da
bi zaznavali ali odstranjevali viruse, črve in ostalo nesnago, preprečujejo pa lahko komunikacijo okuženega računalnika z omrežjem ostalih okuženih računalnikov. Vendar le v primeru, da škodljiva koda požarnega zidu
prej ne uspe onesposobiti. Zato je požarni zid brez dobrega protivirusnega programa praktično nemočen.



Slika 8: Požarni zid[8]

4.6 Kdo piše viruse?

Računalniške viruse lahko pišejo le programerji z dobrim znanjem računalniškega programiranja. Najpogosteje pripadajo eni od naslednjih skupin:

PROGRAMERSKI EKSPERIMENTATORJI - to so programerji na fakultetah ali v

[8] Vir pridobljeno na naslovu: http://www.zero-one-x.co.za/images/firewall.jpg

laboratorijih, v katerih preučujejo računalniške virusi, lahko so tudi hekerji, ki jim je programiranje v užitek, in drugi. če virusi teh izvorov zaidejo v javnost, se to zgodi le pomotoma.

ŠALJIVCI - to so osebe, ki se z pisanjem predvsem zabavajo. Ti virusi so navadno hudomušni in neškodljivi, čeprav jih ob odkritju kake nove tehnike škodoželjni programerji hitro prikrojijo v zelo nevarne viruse.

ŠKODOŽELJNI PROGRAMERJI - njihov cilj je popolno uničevanje podatkov iz različnih vzrokov. Med njimi so najpogosteje odpuščeni programerji, programerji iz vzhodnih držav (predvsem Bolgari in Rusi), ki so pogosto izredno dobro oboroženi z znanjem programiranja. Mnogokrat pišejo takšne viruse tudi pripadniki raznih organizacij (npr. virusi Marihuana, Machosoft, Ho Shi Minh itd.).

MLADI PROGRAMERJI - ti želijo odkriti tehnologijo virusov in niti ne vedo , v kaj se spuščajo. Mnogi med njimi bi se radi s svojim znanjem pokazali pred drugimi. Trenutno je znanih več kot 150 tisoč računalniških virusov in njihovo število stalno raste. Največja sprememba pa ni v vrsti virusov in škodljivih programov temveč v motivih za njihovo pisanje: "Največja sprememba je, da so včasih viruse pisali posamezniki, dandanes pa
jih pišejo kriminalne skupine z namenom zaslužka," je povedal Mikko Hypponen, vodja oddelka raziskovalcev računalniških virusov pri podjetju F-Secure. "In zaenkrat ni videti, da bi se ta trend ustavil. "

Slika 9: Hekerji[9]

4.7 Hekerji

Vdor je posledica bodisi napak na programski opremi:operacijskem sistemu, aktivnih strežnikih programov…bodisi napak pri nastavitvi programske opreme ali napačnega ravnanja uporabnikov. V zadnjem času so najpogostejši vdori posledica klika na datoteko, ki je pripeta v elektronski pošti. Tako je gotovo mogoče vdreti v veliko računalnikov, če pa želi kdo vdreti v točno določen sistem, to bržkone ni prava metoda. Za vdor določene organizacije mora heker zbrati čim več informacij o končnem cilju.

[9] Vir pridobljeno na naslovu:
http://www.dnevnik.si/uploads/image_cache/132c521b710a5cf25e5cbb341a1a179d.jpeg

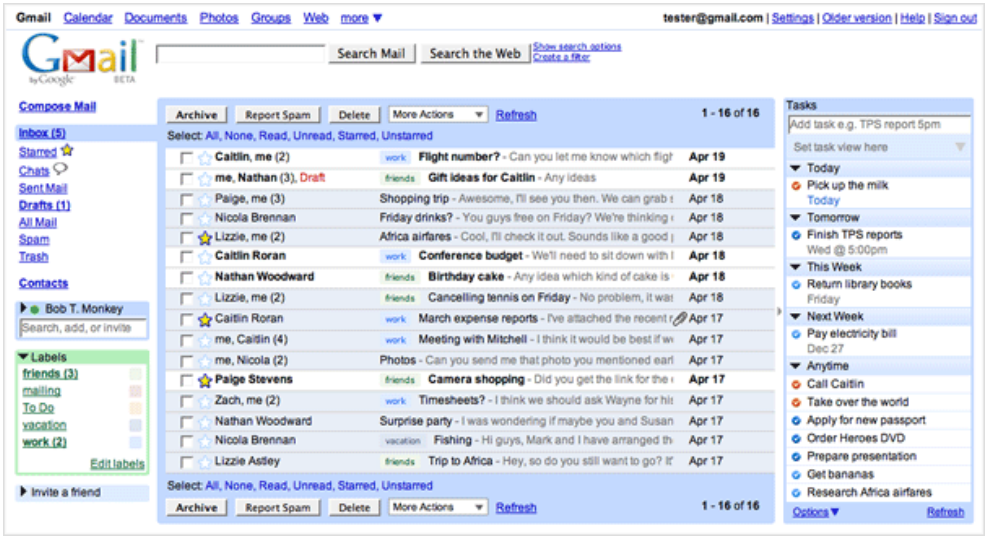
Internet je bogat rudnik informacij za nepridiprave. Spletna stran podjetja je navadno dobra izhodiščna točka. Vdiralci si ogledajo vizitko, natančno ime, lokacijo sedeža in podružnic, kontaktne osebe, telefone…Statistika kaže, da največ vdorov v sisteme podjetij izvedejo zaposleni.

SLEDENJE:

Če si podrobneje ogledamo prvo fazo hekerskega napada. To stopnjo imenujemo sledenje. Za njo hekerji zberejo najosnovnejše informacije o žrtvi. Navadno najprej poiščejo spletne in jih nato shranijo v svoj računalnik in jih analizirajo. V izvirni kodi spletnih strani je pogosto veliko informacij, kot sta Teleport Pro (za okna) in wget(za UNIX), lahko prekopirajo celotno spletno lokacijo v svoj računalnik in jo tam počasi raziskujejo. Nadalje natančno preiščejo splet, tako s splošno znanimi brskalniki, denimo z googlom, kot z naprednejšimi orodji, ki imajo močnejši poizvedeni jezik.

4.8 Kako se ubraniti pred virusi ter v elektronski pošti

Na računalnik namestimo antivirusni program. Ker pa se novi virusi pojavljajo vsak dan, je pomembno, da uporabnik svoj antivirusni program redno dopolnjuje z novimi protivirusnimi vzorci. Današnji protivirusni programi večinoma omogočajo dopolnjevanje virusnih vzorcev prek interneta s pomočjo tehnologije samo posodobitve, kar uporabniku olajša skrb za redno posodabljanje protivirusnih vzorcev. Dobri protivirusni programi so največkrat plačljivi, posodabljanje virusnih vzorcev pa je brezplačno, vendar strošek zagotovo odtehta tveganje okužbe z virusom, s tem pa zmanjša možnost kraje ali izgube podatkov.
Najboljša zaščita pred virusi je pazljivost. Vsa elektronska sporočila ki vsebujejo priponsko, so v osnovi potencialno nevarna, četudi pošiljatelja poznate. Škodljivi programi se v vse večji meri pošiljajo prek okuženih računalnikov in imenika naslovnikov, ki je shranjen na računalniku.
Ne zaganjajte datotek s končnicami >exe<, >js<, >bs<, >scr<. Le redke izjeme formatov datotek lahko odprete brez skrbi, da bi bile okužene z virusi(npr. datoteke s končnico >txt<, >gif<, >mp3<)
V našem programu za sprejemanje elektronske pošte aktivirajte vse možne varnostne mehanizme. Pridobite si program za zaščito pred virusi. Veliko jih je lahko brezplačno najdete na internetu ali pa jih kupite pri specializiranih ponudnikih. Izberite svoj prosti virusni program in z njim redno preverjate datoteke na računalniku ter elektronsko pošto. Ne pozabite ga redno posodabljati(različica programa)-vsaj enkrat na mesec, po potrebi pa tudi pogosteje, virusne baze pa naj se posodabljajo vsak dan. Priporočamo tudi vklop samodejnih posodobitev.



Slika 10: Virusi in elektronska pošta[10]

4.9 Test anti-virusnih programov

Kot vemo so antivirusni programi danes del skoraj vsakega računalnika, zato smo za vas izvedli primerjave kateremu od le teh je najbolje zaupat. Testiranje smo izvajali z nekaj več kot 300 različnimi virusi in nekaj več kot 30 različnimi antivirusnimi programi, na operacijskem sistemu Windows Xp.

Test je 95%no efektiven, brez sponzoriranja kateregakoli izmed produktov.Vsi vemo da dandanes vsako podjetje hvali svoj izdelek in testi ki se ponujajo kot award reviewi večinoma niso resnični.

Spodaj so podana mnenja na podlagi testov in rezultati po naših 4 mesečnih raziskavah, v raziskavi je sodelovalo devet oseb, od tega štirje programerji ter pet računalniških inženirjev.

[10] Vir pridobljeno na naslovu: http://blog.rememberthemilk.com/img/gmail/ss_gmail.png

Slika 11: NOD32[11]

NOD 32 (ESET)

- + Preprost za uporabo
- + Visoka hitrost skeniranja
- + Močna heuristika
- + Majhni updatei
- - Zelo slaba detekcija trojanskih konjev, ena najslabših nasploh (od 60 najbolj pogostih zaznal le enega)
- - Http scaner povzroča težave pri brskanju po internetu.
- - Pogosto sesuvanje programa
- - Heuristika na čas zmedena, označi dobro datoteko za okuženo in obratno.

Kaspersky 7 (Kaspersky Labs)

- + Zelo dobra detekcija
- + Zelo dobra detekcija trojanskih konjev
- + Redne urne posodobitve
- + Močna heuristika
- + Zaznavanje riskwarea (nadležni programi, joke scene, razni dialerji itd)
- - Visoka poraba sredstev
- - Ne nadzoruje sprememb registra ob zagonu računalnika

F-Prot (Frisk)

- + Izredno majhna poraba sredstev (priporočljiv za starejše mašine)
- + Zelo hiter
- + Dokaj dobra detekcija
- + Redne posodobitve
- - Nima E-mail scanerja
- - Ne nadzoruje registra
- - Ne nadzoruje nenadnih sprememb v računalniku

[11] Vir pridobljeno na naslovu: http://dl.img.qj.net/uploads/files_module/screenshots/26403_nod32ea1.jpg

- - Grd vmesnik

AVG 7.5 (Grisoft)

- + Nizka poraba sredstev
- + Dobra detekcija dialerjev
- - Ne najbolša detekcija nasploh
- - Ne nadzoruje registra
- - Resident Shield (ščit pred virusi) metoda nima skoraj da nobenega pomena, saj virus zazna komaj ob skeniranju
- - Pogosto sesuvanje

AVG 7.5 Free (Grisoft)

- + Majhna poraba sredstev
- - Ne najbolša detekcija
- - Ne nadzoruje registra
- - Pogosto sesuvanje
- - Veliki updatei (okoli 3mb)
- - Ne skenira E-pošte
- - Brez tehnične podpore

Mcafee (Mcafee security)

- + Dobra detekcija trojancev
- + Močna heuristika
- + Lep vmesnik
- + Lahek za uporabo
- + Relativno majhni updatei
- + Detekcija riskwarea
- - Za delovanje so potrebni active x kontrolniki
- - Ne nadzoruje registra ob zagonu računalnika
- - Občasno sesuvanje
- - Nima self-protection metode

Panda Antivirus (Panda Software)

- + Dobra detekcija
- + Nadzoruje register
- + Močna heuristika (ena najmočnejših nasploh)
- + Lep vmesnik
- + Redne posodobitve
- - Zelo visoka uporaba sredstev
- - Za delovanje uporablja dosti procesov
- - E-mail skener je zelo počasen

CA Antivirus 2007 (Computer Associates)

- + Močna detekcija trojancev (ena najbolših sploh)

- + Izredno močna heuristika
- + Lep vmesnik
- + Redne posodobitve
- + Online Virus skener ne ovira hitrosti interneta
- - Ne nadzoruje prispele pošte
- - Ne nadzoruje registra ob zagonu računalnika
- - Javlja napake predvsem če imate nameščen še kakšen drug Antivirus

Bit Defender Free(Softwin)

- + Zadovoljiva detekcija
- + Tehnična pomoč tudi pri free verziji
- - Ne omogoča stalne zaščite (za zaščito potrebna registracija, ki pa je free)
- - Nepotrebna poraba sredstev
- - Za delovanje uporablja veliko procesov
- - Zelo počasen

Bit Defender (Softwin)

- + Dobra detekcija (ena boljših nasploh)
- + Kar dobra detekcija trojanskih konjev
- + Redne posodobitve
- + Močna heuristika
- + Nadzor registra ob zagonu računalnika
- + Takoj odzivna tehnična pomoč
- - Podpira le Win 2000, Xp ter Visto
- - Za delovanje uporablja nepotrebne procese
- - Zelo visoka uporaba sredstev
- - Ne nadzoruje web maila
- - Dokaj počasen
- - Težave, če imate nameščen še kakšen drug antivirusni program

F Secure (F Secure Inc.)

- + Izredno močna detekcija trojanskih konjev
- + Izredno močna detekcija nasploh
- + Za delovanje uporablja kar 3 Engine-e,od Kasperskega,Libro ter Orion, slednja služita predvsem za heuristiko
- + Lep vmesnik
- + Redne posodobitve
- + Hitra tehnična pomoč
- - Izredno visoka poraba sredstev (predvsem pri skeniranju)
- - Počasen

Antivir Free (H+Bedv)

- + Dobra detekcija trojanskih konjev
- + Majhna poraba sredstev
- - Veliki nerodni in predvsem počasni updatei

- - Vmesnik je zastarel
- - Ni tehnične podpore
- - Nima E-mail skenerja

Slika 12: AntiVir[12]

Antivir Pro (H+Bedv)

- + Dobra detekcija trojanskih kojev
- + Majhna poraba sredstev
- + Neprestano skeniranje v ozadju
- + Nasploh dobra detekcija
- + Redne posodobitve
- - Vmesnik je zastarel
- - Veliki nerodni in počasni updatei

Norman Virus control (Norman)

- + Majhni updatei
- + Zadovoljiva sandbox heuristika
- + Hitra tehnična pomoč
- - Izredno slaba detekcija
- - Neredne posodobitve
- - Grd vmesnik
- - Kar težek za uporabo
- - Počasen
- - Nima online skenerja
- - Občasno sesuvanje programa

[12] Vir pridobljeno na naslovu: http://lh4.ggpht.com/zuoxingyu/SKT4QkcNDlI/AAAAAAAADCM/1vrJ_Gg8SLU/s288/Avira%20AntiVir%20Personal.jpg

Avast Free Edition (Alwil Software)

- + Majhni updatei
- + Nizka poraba sredstev
- + Tehnična pomoč
- - Slaba detekcija trojancev (od 60 najbolj znanih in razširjenih prepoznal le štiri)
- - Slaba detekcija nasploh
- - Shield je bolj kot ne za okras
- - Otročji vmesnik

Avast Professional (Alwil Software)

- + Majhni updatei
- + Nizka poraba sredstev
- + Tehnična pomoč
- - Slaba detekcija trojancev, klub generičnemu zaznavanju (od 60 najbolj znanih in razširjenih prepoznal le štiri)
- - Slaba detekcija nasploh
- - Shield je bolj kot ne za okras
- - Otročji vmesnik

Norton Antivirus (Symantec)

- + Dobra detekcija trojancev
- + Firewall
- - Poraba sredstev je dokaj velika
- - Nepotrebni procesi
- - Updatei so zelo veliki in le enkrat tedensko
- - Updateat je potrebno ročno
- - Ne nudi zaščite registra
- - Nima online skenerja

Trend Micro Antivirus + Antispyware (Trend Micro)

- + Izredno močna detekcija trojancev (generično zaznavanje)
- + Zadovoljiva detekcija nasploh
- + Požarni zid
- + Močna heuristika
- + Nadzor registra ob zagonu računalnika
- + Antispyware
- + Hitra tehnična pomoč
- + Redni in hitri updatei
- + Lahek in pregleden
- - Dokaj visoka poraba sredstev
- - Nepotrebni procesi

Threatfire Antivirus Free Edition (Pc-Tools)

- + Dobra detekcija

- + Real time zaščita
- + Močna heuristika
- + Adware/Antispyware zaščita
- + Tehnična pomoč dokaj hitra
- - Porabi dokaj veliko sredstev
- - Počasen

Spyware Doctor with Antivirus (Pc-Tools)

- + Dobra detekcija trojancev
- + Antispyware
- + Redni in hitri updatei
- + Real time zaščita
- + Nasploh dobra detekcija (ena najboljših)
- - Počasen
- - Ogromna poraba sredstev (predvsem pri skeniranju)
- - Povzroča neodzivanje računalnika

Avira Antivirus (Avira)

- + Adware/Antispyware zaščita
- + Nizka poraba sredstev
- + Mail skener
- - Grd vmesnik
- - Zelo slaba detekcija trojancev (ena najslabših nasploh)
- - Zelo slaba detekcija nasploh
- - Ne uporablja heuristike
- - Tehnična podpora se odziva kadar jim zapaše
- - Nima self-protection metode
- - Posodobitve so relativno velike
- - Počasni update serverji
- - Real time scan povzroča sesuvanje programa
- - Zaščita je skoraj da neuporabna, saj virus zazna komaj ob skeniranju
- - Ne spremlja sprememb registra ob zagonu računalnika
- - Dobre datoteke zazna kot “suspicius” sumljive datoteke in jih daje v karanteno

Ashampoo Antivirus (Ashampoo)

- + Dobra detekcija trojancev (generično zaznavanje)
- + Redni updatei
- + Močna heuristika
- + Real time zaščita
- + Lep vmesnik
- + Hitra tehnična pomoč
- - Za delovanje uporablja veliko sredstev
- - Nekoliko zakompliciran za začetnike

A- Squared Anti Malvare (Emsi Software)

- + Izredno močna detekcija trojancev (ena najboljših nasploh)
- + Izredno močna detekcija nasploh
- + Adware/Antispyware zaščita
- + Močna heuristika
- + Anti hacker zaščita
- + Real time protection
- + Hitra tehnična pomoč
- + Lep interface
- + Hiter skener
- - Nekoliko neredni updatei

Zone Alarm Antivirus (Zone Alarm)

- + Firewall
- + Redni updatei
- - Slaba detekcija trojancev
- - Slaba detekcija nasploh
- - Za delovanje porabi veliko sredstev
- - Tehnična pomoč sploh obstaja? Piše že..
- - Skupaj z Win SP2 zadeva povzroča velike težave
- - Počasen
- - Občasne težave z požarnim zidom
- - Sesuvanje
- - Skoraj nemogoče uninštalirat

Bullguard Antivirus (Bullguard)

- + Firewall
- + E-mail skener
- + Web skener
- - Slaba detekcija trojancev
- - Slaba detekcija nasploh
- - Tehnična pomoč se odziva enkrat tedensko
- - Za delovanje porabi veliko sredstev
- - Real time zaščita se rada sesuva
- - Ni heuristike
- - Počasen
- - Msn messenger Live sign assinstanta označi kot Trojan generic? Wtf?

Cogen Antivirus (Cogen Media)

- + Izredno dobra detekcija trojancev
- + Nasplošno zadovoljiva detekcija
- + File shredder
- + E-mail skener
- + Spam filter
- + Simple interface
- + Nadzor registra ob zagonu računalnika
- + Tehnična pomoč se odzove takoj

- + Real time zaščita
- - Updatei so relativno veliki in neredni
- - Za delovanje uporabi kar precej sredstev

5 VIRUSI V PRIHODNOST

5.1 Nevarnost virusov v prihodnosti

Strokovnjaki opozarjajo, da bi virusi in črvi v prihodnosti utegnili napasti tudi mobilne telefone. Prejemanje podatkov prek mobilnika je sicer praktično in vedno bolj razširjeno, obstaja pa vse večja možnost, da bi uporabnik prek telefona v prihodnosti prejemal tudi viruse ali črve, ki bi lahko uničili mobilnik. Prvi takšen program se je pojavil že pred dvema letoma, vendar potencialno nevarni črv z imenom Cabir takrat ni prodrl v svet mobilnih telefonov. Telekomunikacijski strokovnjaki poudarjajo, da ne želijo širiti panike, opozarjajo pa, da bi lahko virusi in črvi v prihodnosti predstavljali velik problem v mobilni telefoniji.

Virusi in črvi predstavljajo največjo nevarnost za t.i. pametne telefone, ki ponujajo vrsto poratlov in funkcij. Zato strokovnjaki uporabnike takih mobilnikov opozarjajo na previdnost pri prenosu programske opreme. In kaj nas čaka v prihodnosti? S pojavom prvih virusov na mobilnih telefonih se je nakazal trend razvoja malware aplikacij tudi za mobilnike. Ti postajajo vse bolj podobni računalnikom po funkcijah, kot po povezljivosti. S pojavom novih storitev se pojavlja posledično možnost njihove zlorabe. Se spominjate, tudi pri računalnikih se je začelo z virusi.

Ker hekerji objavljajo izvorno kodo svojih stvaritev na forumih in spletnih straneh, je logična posledica vedno več izpeljank, ki jih razvijajo drugi povzpetniki, hkrati pa se s tem briše sled do prvotnega avtorja zlobne kode. Hekerji so postali prilagodljivejši in se bodo hitreje odzivali na aktualno dogajanje, e-mail, ki vsebuje povezavo na stran za pomoč z žrtvami naravne nesreče, bo vedno pogosteje poslan na zahtevo hekerja, uporabljajočega metode socialnega inženiringa. Pričakovati je vse večjo komercializacijo hekerske ponudbe, malware se bo ustvarjal na zahtevo, za industrijsko vohunstvo, onemogočanje konkurence, prodaja ali najem botneta je že realnost. Z večanjem internetne pasovne širine se bodo okuženi računalniki uporabljali za distribucijo nelegalne programske opreme. Tudi zlobna koda se bo spopadala med sabo, boljše različice bodo poskušale prevzeti kontrolo nad slabšimi. Malware se bo vse bolj razširjal v šifrirani obliki, kar otežuje njegovo detekcijo in mu daje potreben čas za okužbo računalnika, na koncu pa je treba omeniti še, da bodo hekerji namenili vse več časa za iskanje slabosti v delovanju tistih, ki so jim sovražni; antivirusnih programov in požarnih zidov.

Slika 13: Prihodnost virusov[13]

[13] Vir pridobljeno na naslovu: : http://www.racunalniskenovice.com/images/1/H_MAX_1024x768/lenovo_ideacentre.jpg

6 VIRI

Knjiga: P. Hribar, Računalniški virusi, Založba Flamingo, d. o. o., Ljubljana, 2004, strani 55-120
Deskanje po varnih vodah, Matej Kovačič, Ljubljana, 2000 Safe-si, str. 26-27
Revija: Verdonik Ivan, Pozor, hekerji, Monitor, april 2005, letnik 15, št.4
Spletna stran: pridobljeno dne 24. 10. 2009 na naslovu:
-http://www2.arnes.si/~osmbhajdina3/rom2005/a_virusi/virusi_dl.html
- http://www.sc-nm.com/e-gradivo/OSNOVE/antivirusni_programi.html
- http://ro.zrsss.si/projekti/comp/racopismen/anti-virus/Anti%20virus.html

7 VIRI SLIK

Slika 1: Računalniški virusi in črvi, pridobljeno 6.11.09 na naslovu:
http://files.gsobar.uni.cc/GRADIVA_informatika_omrezja_baze/colos/informatika/INFORMATIKA/RACUNALNISKA_OMREZJA/virusi_crvi_files/image002.gif

Slika 2: Cumputer bugs, pridobljeno 6.11.09 na naslovu:
http://cathylwood.files.wordpress.com/2009/04/computer-virus-bugs-clip-art-thumb3167674.jpg

Slika 3: Računalniški virusi, pridobljeno 23.10.2009 na naslovu:
http://beta.financeon.net/pics/cache_F_/F_1_racunalniski_virus_SHU.1201513002.jpg

Slika 4: Varuje, pridobljeno 23.10.2009 na naslovu: http://varujem.com/slike/trojanec.jpg

Slika 5: Anty-Virus System, pridobljeno 23.10.2009 na naslovu:
http://www.bdtutors.com/marketplace%20images//16AVG_Antivirus_System_logo.jpg

Slika 6: Network Security, pridobljeno 23.10.2009 na naslovu:
http://support.novell.com/techcenter/articles/img/ana1997110106.gif

Slika 7: Širjenje računalniških črvov, pridobljeno 23.10.2009 na naslovu:
http://www.microsoft.com/slovenija/doma/varnost/virusi/zivljenjski_cikel_crva.mspx

Slika 8: Požarni zid, pridobljeno 23.10.2009 na naslovu:
http://www.zero-one-x.co.za/images/firewall.jpg

Slika 9: Kitajski hekerji, pridobljeno 23.10.2009 na naslovu:
http://www.dnevnik.si/uploads/image_cache/132c521b710a5cf25e5cbb341a1a179d.jpeg

Slika 10: Remember The Milk Blog, , pridobljeno 23.10.2009 na naslovu:
http://blog.rememberthemilk.com/img/gmail/ss_gmail.png

Slika 11: NOD32 AntiVirus, pridobljeno 23.10.2009 na naslovu:
http://dl.img.qj.net/uploads/files_module/screenshots/26403_nod32ea1.jpg

Slika 12: Movie share, pridobljeno 23.10.2009 na naslovu: http://lh4.ggpht.com/zuoxingyu/SKT4QkcNDlI/AAAAAAAADCM/1vrJ_Gg8SLU/s288/Avira%20AntiVir%20Personal.jpg

Slika 13: Rast intergriranih računalnikov, pridobljeno 23.10.2009 na naslovu: http://www.racunalniske-novice.com/images/1/H_MAX_1024x768/lenovo_ideacentre.jpg