Poslovno-komercialna šola Celje

**SEMINARSKA NALOGA**

Predmet**:** INFORMATIKA

KAZALO:

[1. UVOD: 3](#_Toc165307079)

[2. RAČUNALNIŠKI VIRUSI 4](#_Toc165307080)

[2.1 ŠTEVILO VIROSOV, KI SO NASTALI V ZGODOVINI 5](#_Toc165307081)

[2.2 KAKO SE ZAŠČITIMO PRED VIRUSI? 5](#_Toc165307082)

[2.3 GROŽNJA IN NEVARNOSTI VIRUSOV 6](#_Toc165307083)

[2.4 KDO PIŠE VIRUSE? 6](#_Toc165307084)

[2.5 KAKO SE ZAVARUJEMO? 7](#_Toc165307085)

[2.6 KAKO SE ŠIRIJO ČRVI IN DRUGI VIRUSI? 8](#_Toc165307086)

[2.7 KAKO UGOTOVIMO ALI IMAMO ČRVA, ALI DRUG VIRUS NA RAČUNALNIKU 8](#_Toc165307087)

[2.8 KAKŠNO ŠKODO LAHKO POVZROČAJO VIRUSI 9](#_Toc165307088)

[2.9 VRSTE VIRUSOV 9](#_Toc165307089)

[3. VRSTE PROTIVIRUSNIH PROGRAMOV 10](#_Toc165307090)

[4. VARNOST RAČUNALNIKA 10](#_Toc165307091)

[5. ZGODOVINA VIRUSOV 10](#_Toc165307092)

[6. ANTIVIRUSNI PROGRAMI 11](#_Toc165307093)

[6.1 KAKO DELUJEJO ANTIVIRUSNI PROGRAMI? 11](#_Toc165307094)

[6.2 ANTIVIRUSNA PROGRAMSKA OPREMA 12](#_Toc165307095)

[7. TROJANSKI KONJI 12](#_Toc165307096)

[7. ZNANI TROJANSKI KONJI 14](#_Toc165307097)

[8. PROTIVIRUSNI PROGRAMI 14](#_Toc165307098)

[9. ZAKLJUČEK 15](#_Toc165307099)

[10. VIRI IN LITERATURA 16](#_Toc165307100)

#

# 1. UVOD:

Pri predmetu INFORMATIKA sem se odločila za seminarsko nalog Računalniški virusi. Tema seminarske naloge je zelo zanimiva, saj veliko izveš na kakšne načine se ti lahko okuži računalnik. V uvodu še nekaj besed o virusu na splošno. Virus predstavlja posebno vrsto računalniškega programa, napisanega z namenom, da uničuje podatke v osebnem računalniku oziroma otežuje delo s programsko opremo, ki je nameščena na osebnem računalniku. 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.

# 2. RAČUNALNIŠKI VIRUSI

Računalniški virusi so računalniški program, ki se je sposoben sam razširjati preko drugih računalniških programov ali dokumentov. Zaradi tega se računalniški virusi obnašajo zelo podobno biološkemu virusu, ki se širi tako, da okuži celice.

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.

Računalniški virusi niso omejeni samo na osebne računalnike z okoljem Microsoft Windows. Obstajajo tudi tudi za razne UNIX/Linux sisteme, operacijske sisteme, ki poganjajo vgradnje naprave, kot so mobilni telefoni ali dlančniki. Zgodovinsko gledano so se prvi računalniški virusi pojavili za velike računalnike, nakar so se pisci virusov, skupaj z večanjem dostopnosti osebnih računalnikov, osredotočili na osebne računalnike.

Računalniški virusi so lahko sprogramirani tako, da se aktivirajo na določen datum. Tak je na primer virus Michelangelo, ki se je sprožil šestega marca 1992 (obletnica rojstva italijanskega umetnika Michelangela) in na ta dan brisal vsebino trdih diskov. Ocenili so, da je virus napadel 5.000-10.000 računalnikov.

Pred virusi se bojujemo s pomočjo protivirusnih programov, požarnih zidov in pravočasnih popravkov programja. Danes ti programi niso več namenjeni samo boju proti virusom, ampak služijo tudi preprečevanju prisotnosti vohunskega programja.

Virusi so samo eden od različnih tipov programov, ki so narejeni z zlobnim namenom. To lahko zmede uporabnike, saj so dandanes virusi veliko manj pogosti, kot so bili včasih. Danes prevladujejo predvsem trojanski konji in črvi.

## 2.1 ŠTEVILO VIROSOV, KI SO NASTALI V ZGODOVINI

|  |  |
| --- | --- |
| 1990 | 200 do 500 virusov oz virulentnih programov |
| 1991 | 600 do 1000 |
| 1992 | 1000 do 7500 |
| 1994 | 4500 do 7500 |
| 1996 | Več kot 10000 |
| 1998 | Več kot 20000 |
| 2000 | Okoli 50000 |

Leta 2003 smo praznovali 20. obletnico odkar računalniški virusi povzročajo probleme uporabnikom računalnikov po celem svetu. Takrat je namreč ameriški študent (**Fred Cohen**) izdelal prvi delujoči računalniški virus in z njim okužil grafični program “VD”, ki je tekel na VAX računalniku. Ta virus se je širil tako, da je okuževal uporabniške datoteke, ko je določeni uporabnik se prijavil na računalnik in pognal program VD. Rezultate svojih raziskav je Cohen predstavil na seminarju o računalniški varnosti **10. novembra leta 1983**

##  2.2 KAKO SE ZAŠČITIMO PRED VIRUSI?

Ne obstaja nikakršen splošen recept za zaščito proti virusom, ki bi viruse kar odpravil. Zato pa obstajajo programi kot je antivirusni program, ki poskušajo viruse čimbolj učinkovito odpraviti.

- Če želimo zmanjšati možnosti okužbe z virusi je priporočljivo:

- nalagati le originalne programe in , ker pri piratskih programih ne vemo (ali pa tudi če vemo) od "koga" smo jih dobili in koliko virusov je lahko imel in jih s tem prenesel tudi na naš računalnik.

- pametno je preiskati tudi CD-je iz katerih zaganjamo programe, pa čeprav CD izhaja iz precej zanesljivega vira. Na primer: reklamni CD-ji, ki jih prilagajo razne revije lahko prav tako vsebujejo viruse, saj nikjer ne piše, da so njihovi računalniki brez virusov.

- ne odpirati priponk pri elektronski pošti, tudi če so predstavljene kot tekstovna datoteka in prihajajo od poznane osebe. Zato preden odpremo sporočilo moramo nujno preveriti z antivirusnim programom, če sporočilo ne vsebuje virusa.

- čimbolj pogosto nadgrajujte oziroma preverjajte ali obstaja novejša nadgrajena zbirka poznanih virusov.

## 2.3 GROŽNJA IN NEVARNOSTI VIRUSOV

- Uničenje podatkov: veliko virusov lahko uniči podatke na računalniških diskih s tem, da jih pobriše

- Okvara podatkov: še večjo škodo kot uničenje lahko povzroči okvara podatkov, to je spreminjanje besed v dokumentih ali spreminjanje številk v preglednicah. Samo pomislite, kakšno škodo bi vam povzročil virus, ki bi v vaših finančnih poročilih vse številke pomnožil s faktorjem, npr. z 0,95.

-: nekateri virusi lahko vaše podatke v računalniku pošiljajo na različne elektronske naslove ali pa omogočijo vdiralcem v računalniške sisteme (hekerjem) vpogled v vaše računalnike in krajo podatkov.

- Izguba kredibilnosti vaše organizacije: če boste poslali virus vaši stranki ali poslovnemu partnerju, bo vaša kredibilnost zagotovo nekoliko ogrožena.

- Izguba časa: najbolj pogost in pri okužbi vedno prisoten vpliv na vaše poslovanje je zagotovo izguba časa, ki ga boste posvetili reševanju težav z virusi.

## 2.4 KDO PIŠE VIRUSE?

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

To so programerji na fakultetah ali v labaratorjih, v katerih proučujejo računalniške viruse, 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 s pisanjem predvsem zabavajo. Ti virusi so navadno hudomušni in neškodljivi čeprav jih do odkritij kake nove tehnike Težko doželjni programerji hitro prikrojijo v zelo nevarne viruse.

**Škodoželjni programerji**

Njihov cilj je popolno uničevanje podatkov it različnih vzrokov. Med njimi so najpogosteje odpuščeni programerji, programerji iz vzhodnih držav, ki so pogosto izredno dobro oboroženi z znanjem programiranja.

**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.

## 2.5 KAKO SE ZAVARUJEMO?

Kako se zavarovati pred virusi:

Zaradi tega se uporabniki pogosto varujejo samo pred določenim tipom zlobnih računalniških aplikacij in so bolj ranljivi za ostale. 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. Računalniški virusi niso omejeni samo na osebne računalnike z okoljem Microsoft Windows. Obstajajo tudi za razne UNIX/Linux sisteme, operacijske sisteme, ki poganjajo vgradne naprave, kot so mobilni telefoni ali dlančniki.

Zgodovinsko gledano so se prvi računalniški virusi pojavili za velike računalnike, nakar so se pisci virusov, skupaj z večanjem dostopnosti osebnih računalnikov, osredotočili na osebne računalnike

ne odpirajte elektronske pošte s sumljivimi priponkami( razne slike, program…)

uporabljajte antivirusne programe, ki sproti preverjajo programe in podatke na vašem računalniku antivirusne programe sproti zamenjujte z novimi, posodobljenimi različicami, ki prepoznajo tudi najnovejše viruse

tudi vsako disketo pred uporabo preverite z antivirusnim programom,

uporabljajte samo licenčno programsko opremo.

##

## 2.6 KAKO SE ŠIRIJO ČRVI IN DRUGI VIRUSI?

Skoraj vsi virusi in večina črvov se širijo, ko odpremo ali zaženemo okuženi program.

Številni najnevarnejši virusi so se najprej razširili v obliki e-poštnih prilog – datotek, ki so poslane skupaj z elektronsko pošto. Ponavadi lahko opazimo, ali elektronska pošta vsebuje prilogo, saj jo označuje sponka za papir. Slike, Wordovi dokumenti in celo Excelove preglednice so le nekatere vrste datotek, ki jih lahko vsakodnevno prejmemo v elektronski pošti.Drugi virusi se lahko širijo s programi, ki jih prenesemo iz interneta, ali z okuženimi disketami, od prijateljev ali celo kupimo v trgovini. Obstajajo tudi manj pogosti načini okužbe z virusom, a večina se okuži z odpiranjem in zagonom neznanih prilog elektronske pošte.

Zaradi tega se uporabniki pogosto varujejo samo pred določenim tipom zlobnih računalniških aplikacij in so bolj ranljivi za ostale. 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. Računalniški virusi niso omejeni samo na osebne računalnike z okoljem Microsoft Windows. Obstajajo tudi za razne UNIX/Linux sisteme, operacijske sisteme, ki poganjajo vgradne naprave, kot so mobilni telefoni ali dlančniki. Zgodovinsko gledano so se prvi računalniški virusi pojavili za velike računalnike, nakar so se pisci virusov, skupaj z večanjem dostopnosti osebnih računalnikov, osredotočili na osebne računalnike.

## 2.7 KAKO UGOTOVIMO ALI IMAMO ČRVA, ALI DRUG VIRUS NA RAČUNALNIKU

Ko odpremo in zaženemo okuženi program, lahko da se okužimo z virusom. Računalnik se lahko upočasni, se preneha odzivati ali se sesuje in ponovno zažene vsakih nekaj minut. Včasih virus napade datoteke, ki jih potrebujemo za zagon računalnika. V tem primeru se lahko zgodi, da pritisnemo gumb za vklop in obstrmite pred praznim zaslonom.

Vse to so splošni znaki okužbe z virusom, čeprav jih lahko povzročijo tudi napake strojne ali programske opreme, ki niso povezane z virusi.

##

# 2.8 KAKŠNO ŠKODO LAHKO POVZROČAJO VIRUSI

**-** zgubo zaradi virusov je težko natančno izraziti v denarju, čeprav je lahko škoda velikanska, ampak za vašo organizacijo virusni napad večinoma pomeni:

- izgubo prihodkov oz. zaslužka zaradi izgube časa, ko računalniški sistem ne deluje;

- izgubo podatkov, podatkov o strankah ali celo in-telektualne lastnine;

- izgubo zaupanja strank ali poslovnih partnerjev

## 2.9 VRSTE VIRUSOV

- **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.

- **Makrovirusi:** postanejo aktivni ob odprtju okuženega dokumenta. Nahajajo znotraj enega ali več makrov v dokumentu. V tem trenutku je število virusov te oblike že zelo veliko in še raste.

- **Spremljevalni virusi** - Virus ustvari izvršilno datoteko z istim imenom ampak z drugo končnico. Na primer : Če imate nek program.exe bo naredil program.com.

Slika

1. slika (največja žarišča virusov na svetu v letu 2006)

# 3. VRSTE PROTIVIRUSNIH PROGRAMOV

- F-prot

- Sophos

- Norton

- Norman

# 4. VARNOST RAČUNALNIKA

Nič ne more zagotoviti popolne varnosti, vseeno pa lahko računalnik zaščitimo s posodabljanjem programske opreme in protivirusne programske opreme.

# 5. 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. Prvi virus **brain** se je najprej razvil v ZDA in ni imel škodljivih efektov.

Prvi virusi so bili namreč povečani neškodljivi (izpisovali so npr. le kakšno sporočilo na zaslonu ), pozneje pa se je začelo pojavljati vse več virusov, ki uničujejo ali spreminjajo podatke. Leta 1993 je bilo zaznanih že več kot 3000 različnih virusov.

Vodilni protivirusni centri v svetu tako zdaj dobijo v analizo okoli 100 novih virusov na mesec.

2. slika (Najbolj razširjeni virusi v zadnjih 12 mesecih)

# 6. ANTIVIRUSNI PROGRAMI

Antivirusni programi nam pomagajo pri prepoznavanju in odstranjevanju računalniških virusov. Programerji računalniških virusov vsakodnevno proizvajajo nove viruse in proizvajalci antivirusnih programov jim vztrajno sledijo. Navadno se že v nekaj dneh na trgu pojavi nova različica antivirusnega programa, ki ga prepozna in uniči.

Antivirusne programe lahko jih poiščemo na internetu ali pri prodajalcih programske opreme.

## 6.1 KAKO DELUJEJO ANTIVIRUSNI PROGRAMI?

Lahko ga uporabljamo samo za posamezno preverjanje disket ali določenih datotek, lahko pa je v stalni pripravljenosti in sproti preverja elektronsko pošto s katerimi delamo.

Ko antivirusni program zazna virus, imamo možnosti:

-program okuženo datoteko očisti

-program okuženo datoteko izbriše

## 6.2 ANTIVIRUSNA PROGRAMSKA OPREMA

Čeprav lahko preventiva precej pripomore k zmanjšanju možnosti okužbe, je za uspešen boj z virusi potrebna učinkovita antivirusna programska oprema.
Sophos, eden od svetovnih vodilnih proizvajalcev antivirusne programske opreme, je razvil zaščito za različne sisteme, prilagojene za različne velikosti organizacij. Informacijsko infrastrukturo lahko razdelimo na štiri nivoje, od katerih vsak potrebuje svojo antivirusno zaščito.

1. Uporabniški računalniki (individualni PC-ji, prenosniki in po-dobno) so najbolj ranljivi del informacijskega sistema, saj so večinoma v rokah navadnih uporabnikov.
2. Datotečni strežniki, tako imenovani serverji, so po številu veliko manjši kot uporabniški računalniki in so tudi veliko bolj pod nadzorom administratorjev.
3. Poštni strežniki, ki skrbijo za pošiljanje in sprejemanje elektronske pošte v organizaciji in so glede tega nekakšna vrata v organizacijo.
4. Zunanje storitve, na primer ponudniki internetnih storitev, ki so povsem v upravljanju zunanjih izvajalcev.

# 7. TROJANSKI KONJI

Trojanski konj je računalniški virus, ki lahko povzroči veliko škode na računalniku. Nadzoruje ga heker. Ti virusi so programi, ki se predstavljajo uporabniku kot nek drug program (na primer računalniška igrica ali odstranjevalec neželenih poštnih sporočil ali kaj podobnega), v resnici pa povzročajo škodo v trenutku, ko jih zaženemo.

Trojanski konji se širijo, ko uporabniki odprejo program, za katerega verjamejo, da prihaja iz koristnega vira. Microsoft uporabnikom pogosto pošilja varnostna opozorila po elektronski pošti, vendar nikoli ne vsebujejo priloženih datotek.

- "Backdoors" (zadnja vrata) - Na okužen računalnik je mogoče dostopati z oddaljenega mesta. Obstaja veliko komercijalnih in nekomercijalnih programov, ki imajo isto funkcijo, razlika je le v tem, da v primeru trojanskega konja uporabnik ne ve zanj.

- "password stealers" (tatovi gesel) - odkodira gesla iz Windows 9x PSW datotek ali iz Windows NT RAS datotek, in jih pošlje tatovom.

- "D.O.S. Tools" (Denial-of-Service) - gre za novejšo podskupino. Ti programi poskušajo blokirati delovanje internetne strani, tako da pošiljajo velike količine paketov ali pa nepravilne zahteve. Zelo poznan primer je na primer : Trojan/D\_O\_S.Trinoo ali Trojan/D\_O\_S.Tfn2k, ki je poskušal blokirati nekatere zelo "velike" internetne strani.

- "Simple Trojans" - povzročajo škodo okuženemu sistemu ob zagonu programa ali kadar je izpolnjen določen pogoj. Zato temu razredu rečejo tudi logična bomba.

Vse tri zgoraj predstavljene kategorije (virusi, črvi in trojanski konji) so lahko združeni v en sam program! Na primer : Win32/Moridin, ki vsebuje vse tri kategorije : virus, ki okuži Win32 izvršilne datoteke in pa Microsoft Word datoteke; črv, ki se širi s pomočjo IRC programov in pa MAPI kompatibilnih poštnih klientov; "backdoor", ki sprejema oddaljene komande (lahko se vodi iz oddaljenega računalnika).

3.slika(Graf največje razširjenosti virusov v zadnjih 90 dneh)

# 7. ZNANI TROJANSKI KONJI

-abckOrifice

-BackOrifice 2000

-Beast Trojan

-NetBus

-SubSeven

-Downloader-EV

# 8. PROTIVIRUSNI PROGRAMI

Kaj počnejo protivirusni programi:

-so v programu

- nastanejo kasneje kot virusi

- pregledajo datoteko na tvojem računalniku (A, C, D…)tudi v notranjih pomnilnikih (RAM, ROM…)

Norton AntiVirus je verjetno eden izmed najbolj poznanih **protivirusnih programov** na današnjem tržišču.

# 9. ZAKLJUČEK

Iz te seminarske naloge sem se naučila nekaj novega. Spoznala sem kaj to sploh je računalniški virus, s čim se pridobi in kako se ga znebimo in kako se zaščitimo pred virusu.

Pri tej nalogi sem imela eno težavo saj nisem našla nobene slike ki bi opisovala računalniške viruse, našla pa sem veliko drugih zanimivih lastnosti virusov, ki je prikazano s sliko.

# 10. VIRI IN LITERATURA

a. )knjiga:

Ljubomir, Kostrevc. Računalništvo in informatika. Ljubljana, september 1999. , strani 125-126

Ingrid, Kragelj. Poslovna informatika. Ljubljana 2004, DZS., strani 23 – 25

b. )svetovni splet:

<http://ro.zrsss.si/projekti/comp/racopismen/anti-virus/Anti%20virus.html>

<http://www.microsoft.com/slovenija/doma/varnost/virusi/predstavitev_virusov.mspx>

<http://sl.wikipedia.org/wiki/Ra%C4%8Dunalni%C5%A1ki_virus>