Kaj je virus?

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.

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.

Čeprav je lahko namen virusov, da uničujejo podatke, so pogosto samo nadležni. Nekateri virusi se sprožijo šele po tem, ko mine doloèen 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.

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.

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.

Kaj je trojanski konj?

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

Znani trojanski konji:

- aBckOrifice
- BackOrifice 2000
- Beast Trojan
- NetBus
- SubSeven
- Downloader-EV

Računalniški virusi

Ko so se pred skoraj dvajsetimi leti pojavili prvi računalniški virusi (prvi je bil leta 1986 virus Brain iz Pakistana), so izzvali pravo senzacijo, zdaj pa smo se že kar navadili na njihov obstoj. Kljub temu ob pojavu njihovih vedno novih in inovativnih tehnik širjenja, ki imajo za posledico masovne okužbe v svetovnem merilu, še vedno pritegnejo veliko medijsko pozornost.

Danes je znanih že več kot 90 tisoč različnih virusov, njihovo število pa seveda nenehno narašča. Pri računalniških virusih se je pomembno vprašati:

- Kaj sploh so računalniški virusi?
- Kakšno grožnjo in nevarnost predstavljajo?
- Kakšno škodo lahko povzročijo?
- Kakšna je najboljša obramba pred njimi?

Kaj je računalniški virus ?

Računalniški virus je program, ki se lahko širi preko računalnikov in omrežij z repliciranjem samega sebe, ponavadi brez uporabnikove vednosti. Nekateri virusi prinašajo uničujoče posledice, vsi pa uporabljajo sistemske vire (pomnilnik, procesorski čas, prostor na disku itd.). Z besedo virusi ponavadi zajamemo tudi črve in trojanske konje, ki so v zadnjem času zelo razširjeni. Črv se od virusa v klasičnem smislu razlikuje v tem, da za svojo širitev ne rabi nosilca, to je, da se prilepi na kakšen program, ampak ima svoj samorazmnoževalni mehanizem. Trojanski konj pa je program, ki obljublja nekaj drugega, kar pravzaprav dejansko počne, npr. priponka v elektronski pošti, ki obljublja, da je najnovejši popravek programske opreme, v resnici pa pobriše podatke na disku.

Kakšno grožnjo in nevarnost predstavljajo?

- 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.
- Kraja intelektualne lastnine: 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.

Kakšno škodo lahko povzročajo virusi?

Izgubo 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, npr. finančnih, podatkov o strankah ali celo in-telektualne lastnine;
- izgubo zaupanja strank ali poslovnih partnerjev

Kakšna je najboljša obramba pred virusi?

Zelo pomembna je preventiva, saj je preprečiti vedno lažje kot zdraviti. V postopke preventive spada antivirusna politika z načrtom akcije v primeru napada in izobraževanje uporabnikov. Uporabnike računalnikov moramo poučiti:

- da ne presnemavajo programov ali dokumentov z interneta;
- da uporabljajo Wordove datoteke s končnico rtf namesto doc, ker s tem preprečijo izvajanje makrov in s tem možnost okužbe z ma-krovirusi;
- da ne odpirajo datotek z dvojnimi končnicami (npr. jazsemvi-rus.txt.vbs)
- da ne odpirajo priponk elektronske pošte, če niso povsem prepri-čani o njihovi verodostojnosti;
- da vprašajo računalniškega strokovnjaka za nasvet, če so kakorko-li v dvomu.

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.

Sophos za prva dva nivoja ponuja programsko opremo Sophos AntiVirus, ki neprestano ščiti računalnike – v realnem času, na zahtevo ali po urniku. S svojo inovativno tehnologijo InterCheck omogoča preverjanje ob minimalni porabi sistemskih virov. Po številnih testih velja Sophos AntiVirus za enega najbolj zanesljivih in tudi najhitrejših iskalcev virusov. Nadgrajuje se popolnoma avtomatsko preko interneta, za centralno upravljanje in nadzor pa je v licenco vključen poseben program SAVAdmin.

Za tretji nivo Sophos ponuja MailMonitor in PureMessage, ki vsebuje še antispam, to je zaščito pred nezaželeno elektronsko pošto. MailMonitor in PureMessage ščitita na vratih, to je pri samem vhodu elektronske pošte v organizacijo. To je zelo pomembna točka, saj virusom tu lahko preprečimo nadaljnjo okužbo uporabniških računalnikov in datotečnih strežnikov. S temi programi se lahko izvaja tudi zelo dobra splošna antivirusna zaščita, saj z njimi lahko določimo, da se zavrne vsa elektronska pošta s priponkami izvršilne kode, s priponkami z dvojno končnico in podobno ter se s tem lahko poleg znanih zaustavijo tudi novi, še neznani virusi.

Za zadnji, četrti nivo ponuja Sophos SAVI (Sophos AntiVirus Interface), ki se lahko poveže z različnimi aplikacijami, požarnimi pregradami itd. in skrbi za izjemno hitro preverjanje elektronske vsebine na primer pri ponudnikih internetnih storitev.

Sophos ima na voljo tudi odlično tehnično podporo, organizira pa tudi izobraževalne seminarje v zvezi z zaščito pred virusi.

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**.

Kmalu zatem so prišli na “tržišče” prvi virusi, ki so živeli v DOS operacijskem sistemu na IBM-ovih osebnih računalnikih. Prvi širše znani računalniški virus je bil “**Brain**”, ki se je pojavil leta **1986** in to v **Pakistanu**. Bil je napisan z namenom, da njegovi avtorji ugotovijo kam vse se njihovi programi piratizirajo. To je sprožilo naval dosovskih virusov (Lehigh, Jerusalem, Cascade, Miami...). Ti virusi so se kopirali preko računalniških disket in programja, ki se ga je kopiralo nanje. Zato so bili v primerjavi z današnjimi bolj rariteta. Seveda izjema so bili uporabniki piratske opreme, kjer so virusi uživali nek poseben status. To se lahko spomnijo vsi ljudje, ki so bili računalniško pismeni na začetku 90-tih let.

Kakor so se razvijali antivirusni programi, so se tudi virusi. Nove verzije so imele možnost spreminjanja samega sebe, tako da jih antivirusi niso našli (za kratek čas). Najbolj znani med temi virusi je bil **Michelangelo**, ki je leta **1992** povzročil medijsko histerijo. Na poročilih so napovedovali sesutje vseh računalnikov dne **6. marca**, ampak od tega je bilo bore malo. Mimogrede, ta virus je takrat dejansko uničil večino podatkov na disku in to je bil razlog vse te histerije.

S prodorom MS Oken, so se pisci virusov modernizirali in iz temnega okolja računalniških konzol prešli na pobarvana okna Worda. Nastali so prvi t.i. Makro virusi. Ti virusi so bili napisani v makro jeziku worda, katerega namen je bil avtomatizacija pisanja dokumentov, ampak ker je bil jezik preveč močen in je omogočal neposreden dostop do računalniške opreme, je bil tudi idealen za ustvarjanje virusov. **Makro virusi** so se širili bolj hitro in obsežno kot ostali, ker so ljudje dokumente bolj pogosto kopirali kot same programe.

Medtem, ko so se MS Okna razvijala in vklapljala nove tehnologije vase, so te virusi te tehnologije vedno bolje uporabljali. Znan je recimo **Melissa** virus, ki je marca leta **1999** sprožil nov trend, kjer je makro virus dostopal do adresarja outlook-a in preko njega odposlal sebe vsem znanim ljudem. Večina naslednjih virusov je izkoriščala podobne napake in šibke točke tega operacijskega sistema.

Od leta 2000 imamo skoraj vsako leto vsaj en velik virulentni izbruh, ki se manifestira in potuje preko Interneta. Leta 2000 je to bil Love Bug, ki je napolnil pošto marsikaterega strežnika z "ljubezenskimi pismi", zatem sta prišla še **Nimda** in Code Red.

Zadnji napadi so bili s strani virusov (internetnih črvov) "Sobig", "Palyh", "Slammer" in "MSBlast". Vsi ti virusi so izkoriščali napake v MS Oknih in povzročili škodo, ki si jo pisci virusov niso nikoli predstavljali.

Posredna škoda je bila tudi zaradi "pametnih" administratorjev nekaterih poštnih strežnikov, ki so dodali nanje antivirusne programe, kateri so za vsak sprejeti virus posredovali sporočilo z opozorilom o okužbi naslovniku in pošiljatelju. S tem so povzročili še večjo obremenjenost samih strežnikov in celotnega omrežja (dvojni promet).

Za konec pa še malo statistike. Točnega števila virusov se ne da določiti, tudi zato, ker se nekateri virusi spreminjajo med kopiranjem. Tako nekateri štejejo "družino virusov" kot en virus, drugi preštejejo vse variante tega virusa. Okvirno pa naj bi se število virusov skozi čas gibal takole:

1990 – 200 do 500 virusov oz. virulentnih programov
1991 – 600 do 1000
1992 – 1000 do 2300
1994 – 4500 do 7500
1996 – več kot 10 000
1998 – več kot 20 000
2000 – okoli 50 000

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

2003 – okoli 60 000

Število aktivnih virusov je seveda mnogo nižje in se giblje **okoli 180 vrst oz. družin** virusov. Od teh je mesečno aktivnih manj kot 20. Živo statistiko si lahko pogledate na http://www.f-secure.com/virus-info/statistics/.

Kaj je Virus?

Virus je računalniški program, ki kopira sam sebe.

Kdorkoli misli, da so virusi delo hudobnih in genijalnih programerjev se moti. Virusi so večinoma delo povprečnih programerjev, ki si po zaslugi interneta lahko med seboj izmenjujejo izvorno kodo, razna mnenja, novosti itd. To je tudi razlog, da se pojavi več različic istega virusa v zelo kratkem času (npr. virus WIN95/CIH. Sedaj obstaja že približno deset inačic tega virusa in ostalih, ki temeljijo na njem, samo zato, ker je avtor virusa objavil izvorno kodo in jo je zato lahko uporabil vsak zainteresiran programer.) Potem so tudi programerji, ki uporabljajo le določene dele virusnega programa (oz. procedure/rutine) pri pisanju novih virusov. Zato se tudi pojavlja vsak dan veliko novih virusov in naša naloga je da se pred njimi zaščitimo.

Virus je program, ki lahko kopira sam sebe. Na primer : Virus za izvršilne datoteke (.exe) bo poskušal okužiti tudi ostale izvršilne datoteke na disku, ko bo zagnan z okuženim programom.

Črv (Worm) je program, ki se kopira skozi sisteme. Na primer : I_Worm/Happy se širi z uporabo elektronske pošte. Kadar nek uporabnik pošlje elektronsko pošto in je okužen s tem virusom, se I_Worm/Happy pripne na sporočilo in na tak način širi na druge sisteme. Obstaja več vrst črvov, ki so razdeljeni glede na način širjenja:

- I_Worm uporablja za širitev elektronsko pošto
- mIRC_Worm, pIRC_Worm, vIRC_Worm - uporabljajo za širitev IRC
- network worms (mrežni črvi) - iščejo sisteme, ki jih lahko okužijo preko lokalne mreže ali pa naključne računalnike, ki so povezani preko interneta.

Trojanski konji (Trojans) so programi, ki pridobijo dostop do računalnika na račun lažne identifikacije in ustvarijo nezaželjene stranske učinke. To skupino lahko razdelimo v naslednje podskupine:

- "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).

Če gledamo cilj virusa, jih lahko razdelimo na več kategorij: (ni pa nujno, da ima virus le en cilj. Virusi, ki imajo več ciljev se imenujejo "multipartite" virusi).

1. Boot **virusi** - za širitev rabijo boot (ali zagonski) sektor disketnih enot ali MBR (Master Boot Record) na trdih diskih. Edini način za širitev teh virusov je nalaganje (ali "booting") z okuženih diskov. Dostop in kopiranje okuženih diskov ni nevarno le, če nismo zagnali sistema z okuženega diska. Namig : V BIOS-u spremenite zaporedje "bootanja", tako da disketna enota ne bo prva. Na ta način boste zaščiteni, če boste po pomoti pozabili okuženo disketo v disketni enoti. "Bootanje" z disketne enote je obvezno le kadar inštalirate ali deinštalirate nek operacijski sistem ali pa še v kakšnih drugih posebnih primerih. Ko naredite sistemsko disketo (=disketa s katere je možen zagon operacijskega sistema), je pametno disketo preiskati z antivirusnim programom in jo fizično zaščititi z proti zapisno zaščito (write protection).
2. **Parazitni virusi** - okužijo izvršilne datoteke, tako da ko se izvršilna datoteka zažene, prevzame virus nadzor. Ponavadi se zaženejo pred zagonom izvršilne datoteke in nato kontrolo vrnejo izvršilni datoteki, ki se v večini primerov izvrši normalno kot, da virusa ni. So tudi virusi, ki dobijo kontrolo po izvršeni izvršilni datoteki ali pa ko se izvši določena rutina iz te izvršilne datoteke. Ta tip virusov je težje zaznati, vendar je pa tudi manj razširjen na račun težavnosti. Zato, ker ti virusi okužijo izvršilne datoteke se lahko širijo skozi vsak prenosni medij : disketno enoto, CD, modem, lokalna mreža... Virus se širi, ko se izvrši gostiteljeva datoteka. Parazitni virusi so lahko pomnilniško-obstojni ali neobstojni (memory-resident/nonresident). Če so obstojni potem okužijo vse druge aktivne datoteke. Če pa so neobstojni potem okužijo nekaj datotek in vrenjo kontrolo izvršilnemu programu. Parazitni virusi morajo znati ločiti med že okuženimi datotekami in neokuženimi datotekami. Če virus tega ni zmožen narediti (določene različice virusov Jerusalem in Vienna) potem bo ponavljajoč okuževal neko datoteko, katere dolžina se bo večala in virus bo zlahka zaznan. Namig : Kadar opazite, da so se programi sumljivo povečali uporabite antivirusni program. Ker pa se virus lahko pritaji (stealth virusi) je pametno zagnati antivirusni program iz diskete.
3. **Spremljevalni virusi** - Virus ustvari izvršilno datoteko z istim imenom ampak z drugo končnico. Na primer : Če imate nek program.exe bo naredil program.com. Operacijski sistem, da vedno prednost končnici (.com) in tako se bo izvedel virusni program. Če opazite vedno več takih datotek gre zelo verjetno za okužbo s spremljevalnim virusom.
4. **Povezovalni (Link) virusi** - So izjemno nevarni zato, ker uporabljajo drugačno metodo okuževanja. Ne spremenijo vsebine izvršilne datoteke, ampak spremenijo strukturo imenika (directory structure) in preusmerijo vnos imenika okužene datoteke na področje, ki vsebuje virusno kodo. Ko se izvede virusni program, lahko naloži izvšilno datoteko, poznavajoč pravilen datotečni vnos izvršilnega programa. Odstranjevanje takih virusov iz sistema je težko in tvegano.
5. **Macro virusi** - se nahajajo znotraj enega ali več makrov v dokumentu. V tem trenutku je število virusov te oblike že zelo veliko in še raste (več kot 6000 avgusta 2000).
6. **Virusi, ki okužijo sistem** - ne spremenijo MBR vsebine ali boot sektorja ampak delno spremenijo FAT porazdelitev datoteke IO.SYS (ali ekvivalentnega IBMBIO.COM) z namenom, da vključijo zaporedje virusne kode na začetek te datoteke. Zato, ker DOS (Disk Operating Sistem) bere datoteko IO.SYS sekvenčno se naloži virusna koda prej kot koda datoteke IO.SYS. Če na primer odpremo v navadnem tekstovnem urejevalniku datoteko IO.SYS bo vse izgledalo normalno, zato ker FAT porazdelitvena veriga vsebuje pravilno zapisano področje, ki je bilo spremenjeno s strani virusa.

7 **"Multipartite" virusi** - Tej virusi kombinirajo dva ali več osnovnih tipov virusov opisanih zgoraj. Imamo na primer viruse, ki so zmožni okužiti izvršilne datoteke in Word datoteke ali viruse, ki so zmožni okužiti izvršilne datoteke in boot sektorje, itd.

Kaj lahko virus naredi?

Nekateri virusi so samo zoprni nekateri pa izredno nevarni. Najmanj kar lahko naredijo je to, da vam povečajo velikost datotek in upočasnijo delovanje računalnika. Veliko virusov je tudi takih, ki se samo širijo in ne povzročajo nobene drugačne škode računalniku. Obstaja seveda tudi možnost, da tak "blag" virus občasno sodeluje z določenimi programi in povzroča škodo računalniku. Nekateri virusi so pa veliko bolj škodlivi. Taki virusi recimo namenoma izbrišejo, spremenijo ali kako drugače uničijo vaše podatke ali pa celo formatirajo sistem. Dokler se ni pojavil virus Win95/CIH, je bilo vzeto kot, da virusi ne morejo poškodovati strojnih komponent (hardware components). CIH je bil prvi in na žalost ne zadnji virus, ki je lahko spremenil Flash BIOS, tako da računalnik ni deloval ne glede kolikokrat smo ga zagnali. Še en virus, ki je zmožen okvare strojne opreme (ampak na čuden način) je {Win32,W97M}/Beast. Ta virus se sproži ponoči in namenoma dve uri brez prestanka odpira in zapira vrata CD-ROM enote (to sigurno lahko škodi enoti).

Kako se zaščitimo pred virusi?

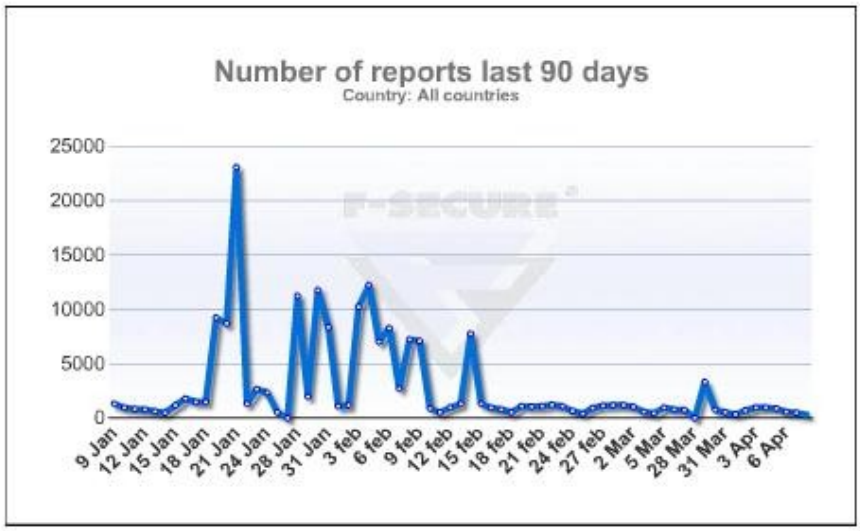
Ne obstaja nikakršen splošen recept za zaščito proti virusom, ki bi viruse kar odpravil. Zato pa obstajajo programi kot je antivirusni program, ki poskušajo viruse čimbolj učinkovito odpraviti. Če želimo zmanjšati možnosti okužbe z virusi je priporočljivo:

- nalagati le originalne programe in ne piratskih, 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 zaneslivega 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. Na primer : VBS/Loveletter, se pripne in pošlje vsem poznanim osebam, ki jih imamo v knjižici z naslovi (address book). 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.

Pojavil se je prvi računalniški virus, ki lahko okuži mobilni telefon. Iz agencije Kaspersky Labs za razvoj antivirusne tehnologije so sporočili, da virus do sedaj še ni imel nikakršnih škodljivih učinkov. Virus, ki se imenuje Cabir, naj bi po nepovsem zanesljivih podatkih razvila mednarodna skupina raziskovalcev, specializirana za ustvarjanje virusov, s katerimi se preverja varnost in zaščita računalniške tehnologije pred škodljivimi napadi. Virus Cabir okuži operacijski sistem Symbian, ki ga uporabljajo številni ponudniki mobilne tehnologije, kot je na primer Nokia, prav tako se lahko širi preko nove brezžične tehnologije Bluetooth. Če virusu uspe prodor v telefon, se na zaslonu pojavi zapis "Caribe", aktivira pa se ob vsaki vključitvi telefona. Sposoben je natančno pregledat informacije telefona, ki za delovanje uporablja tehnologijo Bluetooth in poslati svojo kopijo prvemu naslovniku, ki ga najde.

Odkritje Cabira na podlagi antivirusnega software razvoja F-Secure je dokaz, da imamo tehnologijo, s katero je mogoče ustvariti viruse tudi za mobilne telefone. Strokovnjaki pa že nekaj časa opozarjajo, da se bodo virusi mobilnih telefonov razmnožili in povzročili precejšno škodo.

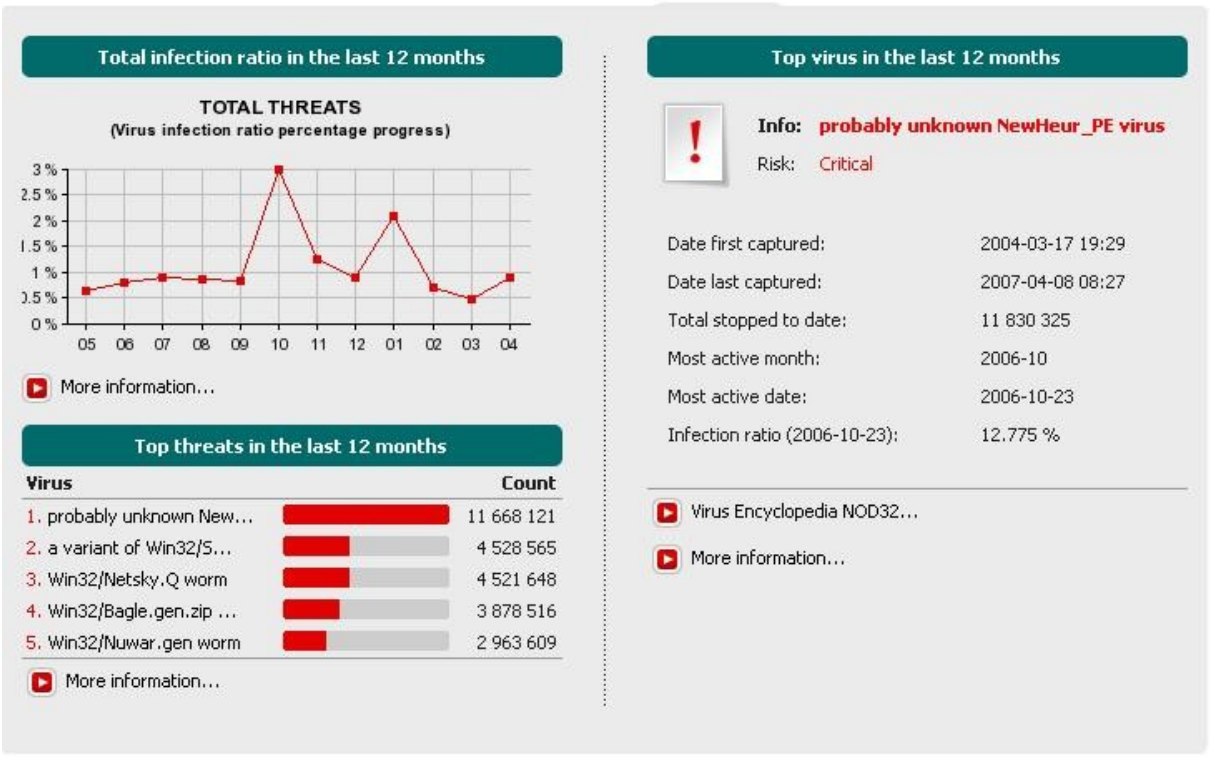
Graf največje razširjenosti virusov v zadnjih 90 dneh.



Največja žarišča virusov na svetu v letu 2006.

http://www.f-secure.com/security_center/virus_world_map.html

Najbolj razširjeni virusi v zadnjih 12 mesecih.



http://obala.net

www.g-7.si

www.secpoint.si

http://www.virusradar.com/index_c12m_enu.html

http://www.nod32.si/