RAČUNALNIŠKI VIRUSI

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 (virusi, ki se zaženejo na določen datum). Do nedavnega so se virusi prenašali v glavnem preko disket (piratske kopije programov, igrice, preiskusni programi).

Z razvojem Interneta pa se virusi danes prenašajo in okužujejo računalnike - magnetne medije s pomočjo elektronskih sporočil, ki so jim pripeti virusi v obliki priloženih datotek, oziroma preko drugačnih načinov izmenjave podatkov.

Virusi večinoma napadajo ukazne datoteke (bat, exe, com, sys), kar ima za posledico nepravilno delovanje programov ali celo izgubo podatkov zaradi sprememb, nastalih v ukaznih datotekah, ki so spremenile lastnosti "originalnih" datotek. Vse bolj pa se "uveljavljajo" MACRO virusi, ki se širijo preko dokumentov, napisanih naprimer z urejevalnikom besedil (Winword).

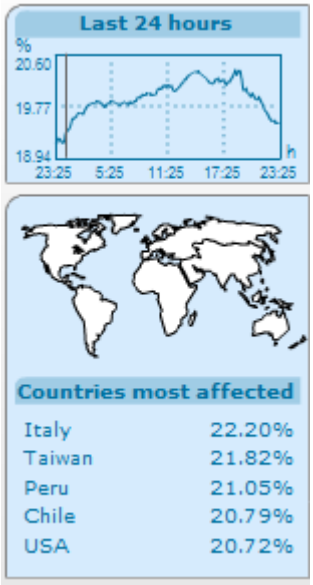
VRSTE VIRUSOV
Viruse lahko razdelimo v tri osnovne skupine:

- 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.

- Makro virusi: postanejo aktivni ob odprtju okuženega dokumenta.
Bolj podrobno pa lahko viruse razdelimo še na:

-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.

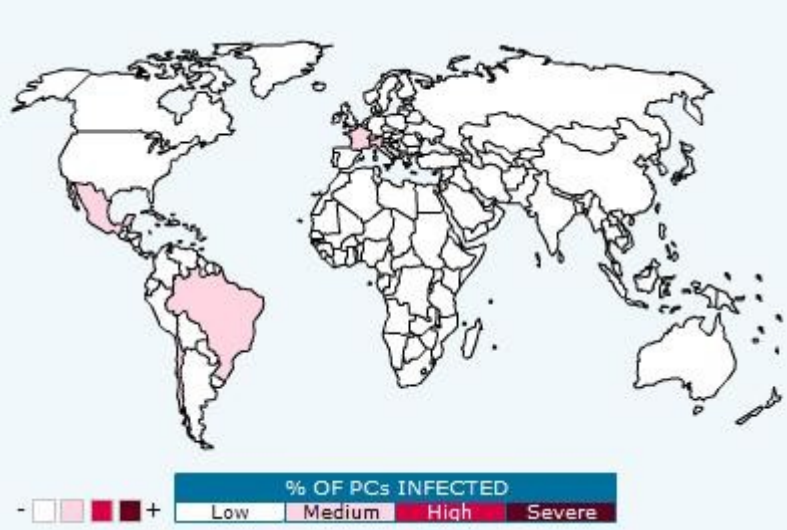
- Link viruses - povezovalni virus - deluje tako, da poveže v prvi točki direktorija (mape) eno ali več izvršilnih datotek v enotno skupino, povezano z virusno kodo. Originalna koda skupine se shrani v neuporabljen del mape, tako,da z zagonom programa sprožimo tudi delovanje virusa.

- Macro viruses - deluje tako, da izbriše ali spremeni obstoječe makro ukaze v programu, s tem pa povzroči nepravilno delovanje posameznega programa (naprimer Winword).
Pred delovanjem virusov se zaščitimo s programi, ki odkrivajo, odstranijo in preprečujejo okužbo z računalniškimi virusi.
Imenujemo jih antivirusni programi (F-PROT, VIRUS SCAN...).
Zaradi nastajanja vedno novih virusov antivirusni programi hitro zastarajo.

Zaščita pred virusi :

- z uporabo najnovejših verzij antivirusnih programov,
- z uporabo originalnih verzij programov,
- z obveznim preverjanjem sposojenih magnetnih medijev (disket) z antivirusnim programom,
- s preverjanjem trdega diska-ov pred uporabo računalnika z antivirusnim programom.

Trenutno številko okuženih računalnikov ni mogoče izvedeti, saj se virusi širijo 24ur na dan.
Spodaj si lahko pogledate tabelo okužnosti računalniških virusov po celinah:



Znaki okužbe z virusom:

Napogostejši znaki nepravilnega delovanja računalnika zaradi okužbe z virusom:
- 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, oziroma blokada pri izvajanju le-teh,
- disketna enota ne deluje,
- zvočni efekti,
- opracijski sistem se ne naloži,
- sporočilo o pomanjkanju "spomina",
- izbrisani "makro ukazi",
- počasno delovanje računalnika

Antivirusni programi:

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.

Position	Virus	Percentage of reports
1	W32/Zafi-D	25.3%
2	W32/Netsky-P	17.5%
3	W32/Sober-N	10.3%
4	W32/Zafi-B	4.7%
5	W32/Netsky-D	3.8%
6	W32/Mytob-BE	2.6%
7	W32/Netsky-Z	2.3%
8	W32/Mytob-AS	2.0%
9	W32/Netsky-B	1.9%
10	W32/Sober-K	1.7%
Others		27.9%

Računalniški virusi niso omejeni samo na osebne računalnike z okoljem Microsoft Windows. Obstajajo tudi 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.

Glavne tarče virusa so ponavadi programske datoteke, katere so namenjene večjim dejavnim procesom. Druge večje datoteke in listine se lahko okužijo tudi preko spleta.