PROGRAMSKI VSILJIVCI

Programski vsiljivci so računalniški programi, katerih izključni namen je povzročanje škode. Prvi (računalniški) virus naj bi bil Creeper (v zgodnjih 70-tih letih), sredi 80-tih pa so se že pojavili programski vsiljivci, ki so se znali razmnoževati med sabo. Trenutno je znanih okoli 200.000 različnih vrst programskih vsiljivcev, dnevno pa se v povprečju pojavi več kot 40 novih. Tarča napadov so v večji meri sistemi na katerih je nameščeno okolje Windows.

Računalniška virologija deli klasične računalniške vsiljivce na trojanske konje, bombe, zajčke, črve in viruse. Med sodobnejše vsiljivce pa štejemo neželeno oglaševanje - spam in potegavščine.

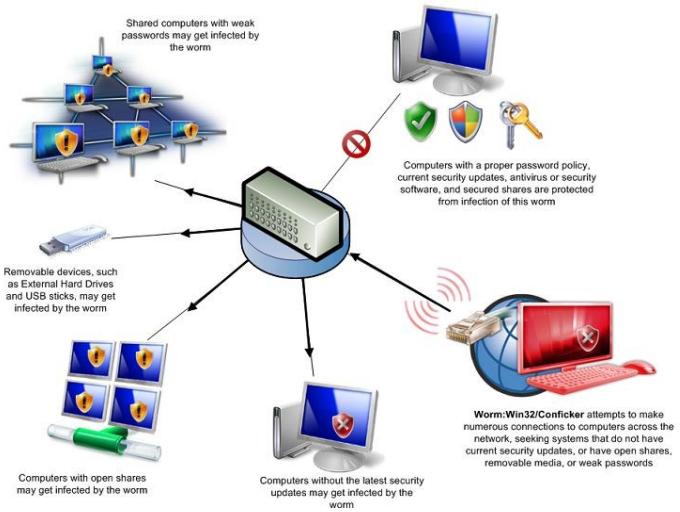
KLASIČNI RAČUNALNIŠKI VSILJIVCI

Slika 1: Računalniški virus (http://mekundan.blogspot.com/2011/05/computer-virus.html)

- **Trojanski konj** je virus, ki lahko povzroči veliko škode na računalniku. Ime je dobil iz bitke pred Trojo. Nadzoruje ga heker. Ti virusi so programi, ki se predstavljajo uporabniku kot neki drug program (na primer računalniška igrica), v resnici pa povzročajo škodo v trenutku, ko jih zaženemo. Torej to pomeni, da na skrivaj izvedejo neko drugo, računalniku škodljivo opravilo.
- **Bomba** je zlonamerni program, ki čaka v računalniku, dokler se ne izpolnijo določeni pogoji, nato napade. Na računalnik jih uporabnik zavestno prenese, vendar on tega ne ve.
- **Zajček** se v računalniku nenadzorovano množi in ga tako upočasnjuje. Na računalnik se prenese sam in išče nove računalnike da jih okuži. Zasede pomnilnik ter obremenjuje trdi disk.
- **Črv** je zelo podoben zajčku, vendar ta okuži vse računalnike v določenem omrežju in ne le enega.
- **Računalniški virus** je najbolj zapletena oblika računalniških vsiljivcev, ki se je sposobna razmnoževati in prenašati v računalniku brez vednosti in volje uporabnika. Virus najprej poišče neokužen program v računalniku in ga okuži. Ko program poženemo, virus spet poišče drug neokužen program in ga okuži …
  Gostitelj virusa je računalniški program oziroma izvršna datoteka. Med razmnoževanjem in prenašanjem se začasno naseli tudi v ostale dele pomnilnika (slikovne datoteke, sistemski del trdega diska,…).Razen uničevanja podatkov, lahko virusi povzročajo še druge težave. Pogosto so samo nadležni; na primer izpisujejo sporočila na zaslon. Nekateri virusi se sprožijo šele po tem, ko preteče določen čas od okužbe računalnika ali ob določenem datumu ali ko okužijo zadostno število drugih računalnikov. Virus, ki ne povzroča škode kljub temu troši računalniška sredstva; npr. obremenjuje procesor in zapolnjuje pomnilnik.

PRIMER VIRUSA: Conficker

Virus Confiker je znan tudi kot Downup, Downadup in Kid; je računalniški črv. Cilja na Microsoft Windows operacijski sistem. Uporablja pomanjkljivosti v opremi Windows in napada na administratorjeva gesla. Črva je zelo težko preprečiti saj uporabljajo veliko naprednih tehnik.



Slika 2: Virus Confiker (http://www.microsoft.com/security/pc-security/conficker.aspx)

SODOBNI RAČUNALNIŠKI VSILJIVCI

- **Spam** je nezaželeno oz. nadležno sporočilo, ki je poslano večjemu številu naslovnikov z namenom vsiljevanja vsebine, ki se je naslovniki sami ne bi odločili prejemati. V veliki večini primerov gre za oglaševanje plačljivih storitev ali izdelkov. Po navadi se s "spam" pošto oglašujejo izdelki ali storitve dvomljive kvalitete, velikokrat pa gre za goljufije. Količino lahko zmanjšamo, da naslov svoje elektronske pošte ne posredujemo vsakomur. Najboljša rešitev proti spamu je nakup programa ANTISPAM.

- **Potegavščina** je sporočilo, ki namerno širi neresnice, svari uporabnike pred namišljenimi nevarnostmi in obljubljajo nagrade. Opozarja na to, da kroži nevaren virus, ki bo izbrisal cel trdi disk, v primeru, da odpremo e-mail sporočilo.

ZAŠČITA RAČUNALNIKA PRED OKUŽBO

Najprej moramo računalnik zaščititi pred okužbo z namestitvijo požarnega zidu in anti-virusnega programa. Moramo pa tudi redno nameščati popravke operacijskega sistema s katerimi krpamo najdene luknje, preko katerih bi lahko vdrli vsiljivci. Zelo pomembno je, da vsak sam uporabnik pazi na varnost s tem, da ne odpira sumljivih datotek in da ne hodi na sumljive strani na internetu. Ne sme odpirati nobenih neznanih elektronskih sporočil, predvsem pa datotek, ki so pripete saj se v teh lahko skriva virus ali trojanski konj. Ob priključitvi zunanjih pomnilnih enot kot so USB ključki, zunanji diski, dvd-ji, cd-ji, pa je le te treba najprej preskenirati z anti-virusnim programom ter ob ugotovitvi okuženosti medij odstraniti ali pa zlonamerno kodo z anti-virusnim programom izbrisati. Zelo priporočljivo je sam operacijski sistem zaščititi z geslom, ki naj bo izbrano tako, da ga je težko ugotoviti.

VIRI

- http://webcache.googleusercontent.com/search?q=cache:XBziPAcV9n0J:www.druga.org/~ftpvaja/1_letnik0607/PredstavitevIzrazov07/1d20/PredstavitevVsiljivci.pps+programski+vsiljivci&cd=8&hl=sl&ct=clnk&gl=si&lr=lang_en%7Clang_sl
- http://www.tretja.si/informatika/1_letnik/vaje/Zgradba%20racunalnika.pdf
- http://www2.grafika.ntf.uni-lj.si/uploads/media/08-Varnost_zasebnost_etika.pdf
- http://ro.zrsss.si/projekti/comp/racopismen/anti-virus/Anti%20virus.html
- …