2008

Rīgas Valsts tehnikums

Oskars Putniņš

[RUNĀJOT PAR PROGRAMMATŪRAS DROŠĪBU...]

Viss, kas būtu jāzina par datorsistēmas kaitēkļiem - vīrusiem, kā arī efektīgākie paņēmieni cīņā ar tiem. + pielikums

Saturs

Viss, kas būtu jāzina par datorsistēmas kaitēkļiem (vīrusiem)

Kas ir Vīruss?

Divos vārdos (Kā strādā vīrusi, kādas ir viņu funkcijas un kā ar tiem var inficēties)

Datorvīrusi ir tikai un vienīgi cilvēka prāta darbības rezultāts.

Datorvīruss ir programma, kas izplatās bez datorlietotāja piekrišanas vai zināšanas, inficējot failus datora cietajā diskā. No viena datora citā tie nokļūst caur tīklu, piemēram, ar e-pasta starpniecību, lejupielādējot nezināmas izcelsmes failus no vienādranga (P2P) failu apmaiņas tīkliem (piemēram, DC++, Bittorent, eMule) vai tiek pārnesti, piemēram, ar USB atmiņu vai kompaktdisku.

Tāpat kā nav konkrētas vīrusu definīcijas, nav arī konkrēta vīrusu klasifikācija. Daži vīrusi ir salīdzinoši nekaitīgi, piemēram, uz datora ekrāna izdrukā kādu paziņojumu, kamēr citi var sabojāt vai pilnībā izdzēst datus no datora cietā diska. Vīrusus var klasificēt pēc ļoti dažādām pazīmēm :

* bīstamības pakāpes
* inficēšanās veida
* garuma
* izvietošanās sistēmā utt.

Lielais vairums vīrusu parazitē konkrētos failos, pievienojot savu ķermeni programmai vai kādam citam konkrētam failam, kas noteikti ir inficējamā sistēmā. Tāpat katram vīrusam ir savas “iemīļotās” vietas sistēmā, kur tas novietojas uzreiz pēc iekļūšanas tajā. Zinot īpašības, kas ir unikālas katrai vīrusu grupai, ir krietni vieglāk tos atklāt un neitralizēt.

Atsevišķi vīrusi tiek saukti par tārpiem, jo pavairojas paši, bez lietotāja iejaukšanās, savukārt trojas zirgi, ir faili, kas pirmajā brīdī liekas nekaitīgi, bet satur ļaundabīgu kodu, ko izpildot ļaundaris var panākt kontroli par lietotāja datoru. Atšķirībā no vīrusiem trojas zirgi neinficē citus failus.

Vīrusi ir sarakstīti ļoti daudz, tāpēc tos visus lai aprakstītu vajag milzums daudz laika. Datorvīrusu sugu kopskaits pārsniedz jau 2.7tūkstošus. Ik dienu rodas vidēji 2 līd 3 datorvīrusu sugas, lai pasargātu savu datoru, to nepieciešams aprīkot ar antivīrusu programmatūru.

Daži vīrusu piemēri:

Word makro vīruss. Tā kā tas var izplatīties ar dokumentu un e-pasta pielikuma palīdzību, šis vīruss ir ļoti izplatīts. Tas neko nebojā, jo jaunā versija ekrānā parāda tikai paziņojumu “Have a nice day!”, tomēr tam uzrodas daudz draudīgāki radinieki. Piemēram, Wazzu jūsu dokumentā var pārkārtot vārdus un dažās vietās iespraust Wazzu. FormatC ir ļoti bīstams Trojan grupas vīrusiem, kas noformatē jūsu cieto disku, tiklīdz jūs atverat inficēto failu.

One Half - vairākdaļu polimorfs, zaglīgs (stealth) vīruss, kas pakāpeniski zagšus šifrē cieto disku. To nevar ievērot, jo tad, kad tiek pieprasīts kāds no kodētiem failiem, vīruss pats to atšifrē. Tad, kad puse no cietā diska ir šifrēta, vīruss paziņo "This is one half" un turpmāk kodētos failus neatšifrē, kā arī no inficētā diska vairs nav iespējams palaist sistēmu. Antivīrusu programmas var iznīcināt šo vīrusu, bet nespēj atšifrēt kodēto informāciju.

Ripper - bīstams boot sektora vīruss, kas pakāpeniski bojā informāciju uz cietā diska. Tā kā tas notiek lēnām, jūs varat arī neievērot šos bojājumus līdz brīdim, kad tie jau kļuvuši nopietni.

Tā varētu turpināt un turpināt aprakstīt vīrusus, bet šie ir biežāk sastaptākie vīrusi.

Kas un kāpēc rada vīrusus?

Vīrusu izstrādātājus iedala trīs grupās. Sākotnēji ar vīrusu rakstīšanu galvenokārt nodarbojās studenti un skolnieki, lai praktizētos programmēšanā. Otro grupu veido datorhuligāni, kuru izstrādātie vīrusi spēj radīt jau nopietnus draudus nepietiekami aizsargātiem datoriem, taču viņu mērķis nebija gūt peļņu, bet gan kaut ko izmainīt vai pat sabojāt. Spilgts piemērs ir t.s. Černobiļas vīruss, kuru izstrādāja 22 gadus vecs jaunietis no Taizemes. Sabojāja datoros esošo informāciju un radīja milzīgus zaudējumus. Pēc diviem gadiem viņu apcietināja par izraisīto datorvīrusa epidēmiju. Savukārt 3. grupas galvenais mērķis ir izstrādāt jaunus vīrusus, kurus nebūtu iespējams identificēt un kuri spētu mutēt. Mūsdienās vīrusu industrija ātri kriminalizējas, līdz ar to tradicionālo vīrusu skaits, kurus rada 1. un 2. grupas pārstāvji, pakāpeniski samazinās. To ietekmē arī vīrusu radītāju aresti, kas viņus attur no riska sekām. Kriminālais bizness, kura pamatā ir nelegāla naudas iegūšana, ir viens no tiem iemesliem, kā dēļ visvairāk tiek izstrādāti tieši «komerciālie» vīrusi. Šo vīrusu darbība rada visnopietnākos draudus svarīgām informācijas sistēmām un arī parastiem interneta lietotājiem.

Datorvīrusi - kriminālais bizness!

Izplatītākie un pirmie vīrusu veidi ir t. s. uz «Trojas zirga» tehnoloģijas bāzētas kaitnieciskas programmas, kuru darbošanās rezultātā datorā uzglabātā informācija (piemēram, interneta banku lietotāju pieslēgšanās vārdi un paroles) tiek nodota svešām personām. Attīstoties šo vīrusu veidiem, parādījās programmas datoru nesankcionētai attālinātai administrēšanai, kas nozīmē, ka ir iespēja piekļūt lietotāja datora resursiem, viņam pašam par to neko nezinot. Taču vairākums «Trojas» programmu ir orientētas uz nesankcionētām darbībām banku sistēmās. 2003. gadā tika reģistrēti pirmie «zombiju» tīkli kā līdzeklis masveida surogātpasta izsūtīšanai. 2000. gadā tika radīti vīrusi, kuri automātiski aktivizē dažādus reklāmas logus, apgrūtinot lietotāja darbu, t. s. *Adware*.

Citas populāras kaitnieciskās programmas nodrošina virtuālās naudas zagšanu, kā arī veic maksas pakalpojumu patvaļīgu aktivizēšanu (kā piemēru

var minēt jaunas vīrusu rakstīšanas tehnoloģijas mobilajiem telefoniem, kad tiek zvanīts uz dārgiem maksas numuriem), tādā veidā piespiežot lietotājus vēlāk atmaksāt notērētos naudas līdzekļus. 2004. gadā populāras kļuva viltoto antivīrusu sistēmas, kuras par noteiktu naudas summu iegādājoties un aktivizējot lietotājiem tiek iegalvots, ka programma sekmīgi veikusi vīrusu identificēšanu un likvidēšanu, taču tā ir tikai klientu maldināšana un labākajā gadījumā datorsistēmā nekādas izmaiņas nenotiek. Kā jaunāko var minēt vīrusu veidu, kurš šifrē informāciju uz datora cietā diska un no informācijas īpašnieka tiek izspiesta nauda par informācijas atšifrēšanu. Tāpat milzīgas naudas summas tiek izspiestas, organizējot tādus uzbrukumus lielu uzņēmumu sistēmām, kas pilnībā paralizē to darbu (*DDoS*). Sistēmas darbs tiek atjaunots, kad ir samaksāta pieprasītā naudas summa.

Attīstot datorvīrusu kriminālo biznesu, tiek organizētas īpašas tirdzniecības vietas, tā sauktie melnie tirgi, kur interesenti var iegādāties noteiktus vīrusus, kas izmanto konkrētas programmatūras vājās vietas. Tāpat tur var nopirkt elektronisko adrešu bāzes un izmantot tās surogātpasta sūtīšanai. Un vēl ir iespēja pat veikt speciālu pasūtījumu noteiktiem mērķiem paredzētu vīrusu izstrādei. Tas kārtējo reizi apliecina to, ka, ja ir pieprasījums, tad būs arī piedāvājums. Diemžēl antivīrusu programmām kļūst arvien grūtāk pretoties jaunajiem vīrusiem. Vienu no bīstamākajām vīrusu tehnoloģijām ir kriptēšana. Jaunajām vīrusu sistēmām, kuras izmanto kriptēšanas metodes, nākotnē jau vairs nebūs iespējams pretoties. Otrā kritiskākā tehnoloģija ir vīrusi, kuros ir iebūvēta pretošanās konkrētām antivīrusu sistēmām. Tās ļauj pilnīgi paralizēt antivīrusa programmas darbību, mainīt antivīrusu uzstādītos parametrus utt. Pieaugot dienā saražoto vīrusu skaitam, drīz var tikt sasniegts līmenis, kad antivīrusu izstrādātāji vairs nespēs pienācīgi reaģēt uz visiem ienākošajiem vīrusiem.

Efektīgākie paņēmieni cīņā ar datorvīrusiem

Kas ir antivīrusu programmatūra?

Divos vārdos (Kā strādā antivīrusi un kādas ir viņu funkcijas)

Antivīrusu programma pārbauda katra faila saturu, meklējot tajā noteiktu koda modeli, kas atbilst tā saucamajai vīrusa definīcijai, respektīvi, kaut kam kas tiek uzskatīts par kaitīgu lietotāja datoram.

Katram failam, kas atbilst vīrusa definīcijai, antivīrusu programmatūra piedāvā vairākas iespējas, piemēram, izņemt no tā ļaundabīgā koda daļu (gadījumos, kad tas iespējams), novietot failu karantīnā vai pilnībā izdzēst no datora cietā diska.

Ik reiz, kad antivīrusu programmu izstrādātāji iegūst informāciju par jaunu vīrusu, tie savai datu bāzei (sauktai par vārdnīcu) pievieno vienu vai vairākas vīrusu definīcijas. Šīs definīcijas iespējams iegūt veicot atjauninājumus. Pēc katras jaunas definīcijas lejupielādes lietotājs var pārbaudīt savu datoru. Šo procesu ieteicams uzstādīt, kā automātisku. Gandrīz visas antivīrusu programmas ļauj sastādīt vīrusu skenēšanas grafiku, piemēram, atstājot datoru ieslēgtu pa nakti, Jūs varat pārbaudi ieplānot laikā no 00:30.

Lielākajā daļā antivīrusu bez failu pārbaudes pēc vīrusu definīcijām papildus ir heiristiskās pārbaude, respektīvi, pastāv iespēja, ka koda fragments failā neatbilst nevienai no vīrusu signatūrām, tomēr tajā ir kāda no iespējamām vīrusa pazīmēm. Heiristiskā pārbaude ļauj lietotājam izsargāties no vīrusiem, kas pagaidām vēl nav definēti.

Antivīrusu programmu piemēri

Grisoft AVG anti-virus
Kasperski Anti-Virus
Panda Software Antivirus
McAfee VirusScan
Norton AntiVirus
u.c.

legādāties antivīrusu nemaz nenozīmē šķirties no lielas naudas summas – internetā tiek piedāvāti arī bezmaksas antivīrusi. Lai noteiktu vai antivīruss ir drošs vai arī ne pārāk drošs ir vairāki kritēriji – viens no tiem ir datu bāžu atjaunošana. Datu bāze sastāv no vīrusu saraksta, ko atpazīst antivīrusa programma un pēc tā cik bieži papildinās šis saraksts ar jauniem kaitēkļiem, var spriest cik efektīgs ir antivīruss. (skatīties tabulā)

Profesionāļu viedokļi un ieteikumi

Uzņēmumi tērē naudu drošības procesiem, instalē antivīrusu programmas un to jauninājumus, un tā ir vistīrākā naudas izšķērdēšana - tā teica *John Stewart*, kurš ir Cisco kompānijas drošības dienesta vadītājs. Uzstājoties AusCERT 2008 konferencē, kura notika Austrālijā, drošības eksperts paziņoja, ka vīrusu izstrādes industrija strādā daudz ātrāk kā antivīrusu ražotāju industrija, padarot neiespējamu datoru lietotājiem palikt drošībā.

Drošības eksperts apliecināja, ka pārāk daudzi uzņēmumi ir iemācījušies sadzīvot ar patstāvīgām datoru vīrusu problēmām. Daudzi uzņēmumi pasaulē uzskata, ka inficēti datori ir viņu biznesa neatņemama sastāvdaļa.

Vīrusu problēmu sakarā eksperts arī norādīja risinājumu – lietot tikai tādas datoru programmas, kuras ir autorizētas un pārbaudītas. Viņš papildināja, ka vieglāk cīņā ar vīrusiem ir izmantot atļauto datora programmu sarakstu, nevis veidot aizliegto, kā tas tiek darīts līdz šim.

Antivīrusu programmu ražotāji gan nepiekrita drošības eksperta viedoklim. Antivīrusu programmas McAfee reģionālais vadītājs *Gavin Struthers* pauda viedokli, ka, lai arī antivīrusu programmu un to jauninājumu instalēšana nav perfekts problēmu risinājums, tā tomēr nav tikai naudas tērēšana.

Cits tehnoloģiju eksperts no CA interneta drošības uzņēmuma, *Chris Thomas* teica, ka antivīrusu programma viena pati nenodrošina pietiekamu datoru aizsardzību. Vīrusu izplatītāji un antivīrusu programmu veidotāji atrodas patstāvīgā sacensībā, apliecināja tehnoloģiju eksperts. Viņš arī atbalstīja Cisco drošības eksperta ideju par atļauto programmu sarakstu, kas varētu būt efektīvāka par aizliegto programmu sarakstu.

Ieteikumi mājas datorlietotājiem:

- Instalējiet **vienu** no antivīrusu programmām
- Regulāri atjaunojiet vīrusu definīcijas un veiciet datora skanēšanu vismaz vienreiz dienā (Šo funkciju iespējams uzstādīt automātiski);
- Pirms kāda faila atvēršanas vai jaunas programmas uzstādīšanas pārbaudiet to. Veiciet vīrusu skanēšanu arī failiem, kas atrodas uz USB atmiņās, CD vai disketēs;
- Pēc failu lejupielādes no interneta, to nekavējoties pārbaudiet.
- Veidojiet vērtīgāko datu rezerves kopijas (vēlams uz CD vai DVD diskiem).

Kā atgūties pēc vīrusu uzbrukuma

Gadījumā, ja vīruss ir nokļuvis uz Jūsu datora cietā diska, ieteicams veikt sekojošas darbības:
- Atslēdziet datoru no tīkla. Pastāv iespēja, ka ļaundaris izmanto vīrusu vai trojas zirgu, lai piekļūtu datiem uz datora vai izmantotu to savu mērķu īstenošanai. Pie tīkla pieslēgts dators var inficēt arī citus datorus.
- Uzstādiet antivīrusu programmu, ja iepriekš tas nav ticis izdarīts, un pārbaudiet datoru. Ja tas nelīdz, mēģiniet vīrusu identificēt un lejupielādēt specifisku tam speciāli paredzētu noņemšanas rīku.
- Mēģiniet nokopēt svarīgākos datus. Esiet uzmanīgi, jo šie dati jāuzskata par potenciāli inficētiem.
- Iespējams, būs nepieciešams pārinstalēt datora operētājsistēmu, tāpēc sazinieties ar speciālistu.

Jaunākie paņēmieni cīņā ar vīrusiem

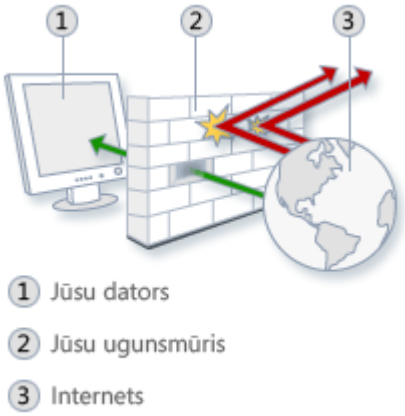
Korejas firma Digiworks gatavojas laist tirgū visai savdabīgus USB atmiņas moduļus ar nosaukumu Virus Chaser, kuru viena no galvenajām funkcijām papildus datu glabāšanai būs vīrusu iznīdēšana lietotāja datorā. Šāda atmiņa, pievienota datoram, sazināsies ar interneta serveri, atjaunos datu bāzi un pārbaudīs datoru, vai tajā nav atrodami vīrusi, Spyware un Adware. Atmiņas modulī jau iepriekš būs uzstādīta programma Bizet Virus Chaser. Korejas tirgū šis produkts nonāks jau šajā mēnesī, bet visā plašajā pasaulē - kādu brīdi vēlāk. Jāatzīst, ka šis risinājums nav radikāli jauns, bet pietiekami interesants, lai tam atrastos pietiekami liels pircēju un lietotāju skaits. Lieka drošība jau nevienam netraucē.

Pielikums

Kas ir ugunsmūris?

Ugunsmūris ir aparatūra vai programmatūra, kura pārbauda informāciju, kas ienāk no interneta vai tīkla, un atkarībā no ugunsmūra iestatījumiem to bloķē vai arī ļauj ienākt datorā. Ugunsmūris var palīdzēt novērst urķu vai ļaunprātīgu programmatūru (piemēram, tārpu) piekļuvi datoram, izmantojot tīklu vai internetu. Ugunsmūris var arī liegt datoram sūtīt ļaunprātīgu programmatūru citiem datoriem.

Ugunsmūris darbībā:



Ugunsmūra darbības ilustrācija

Kā palielināt datora ātrdarbību?

Iedomājaties, ka Jūs ar rokām velkat tukšas ragavas - tā nekas, bet tiklīdz kaut ko pieliekam tikai smukumam vai prieka pēc, tad vilkšana kļūst smagāka, tāpat ir arī ar Windows XP, jo kā jau mēs paši zinām no prakses – Windows XP ir aprīkots ar dažādiem iestatījumiem kas mums nepavisam nav vajadzīgi ikdienas darbu veikšanai, bet katrs no tiem iestatījumiem patērē noteiktu atmiņas daudzumu, kas savukārt samazina Jūsu datora ātrdarbību. Tātad, Jūs varat nopirkt stipri lielāku atmiņu pa kādiem Ls 20 un uz augšu vai vienkārši noņemt šos iestatījumus:

1) Atslēdzam nekam nederīgos efektus, ko var izdarīt izpildot komandu: Start -> Settings -> Control Panel -> System -> Advanced un sadaļā Perfomance spiežam uz pogas Settings. Tad sadaļā Visual Effects noņemam ķekšus visiem nelietojamajiem efektiem.

2) Atslēdziet programmu ielādi pēc katras datora startēšanas, piemēram, ja ikdienā neizmantojat tildes biroja vārdnīcu, kura ielādējas pēc katras datora

startēšanas reizes, kā arī Skype, ICQ utt. un kamēr visu šo salādē, tas aizņem daudz laika un datora resursus, bet, lai tas tā nebūtu, tad ejam: Start -> Run -> msconfig tad pārejam uz sadaļu startup, kur arī noņemam ķekšus no programmām, kuras ne vienmēr izmantojam.

3) Noņemam nevajadzīgas Windows komponentes, ko izdarām pēc komandas izpildes: Start -> Settings -> Control Panel -> Add or Remove Programms , kur atveram sadaļu Add/Remove Windows Components, tad dialoga logā Windows Components Wizard noņemam ķekšus nevajadzīgajām lietām.

Par datora ātrdarbības palielināšanu www.youtube.com – „ZParks video - Datora higiēna"

Adrese: http://www.youtube.com/watch?v=a8bJMg5vNgg