Kompjuterski virusi, crvi, trojanski konji, rootkits i spyware

U današnjem računarskom okruženju postoji više vrsta prijetnji od maliciosnih software-a koji utiču na računarske sisteme počev od datacentara pa do samih računara. Trenutno su najpoznatiji klasični virusi, crvi, trojanski konji, rootkits, spyware i adware. Generalno definicija kompjuterskog virusa je software koji se može samostalno replicirati od računara do računara te obavljati određene zadatke za koje je programiran kao na primjer brisanje podataka sa diska, enkripciju podataka, oštećivanje sistemskih fajlova i podataka na računarima te druge vrste neželjenih izmjena računarskog sistema. Ima više načina kako se virusu repliciraju, a osnovni je da virus ima pristup pisanja radnoj memoriji računara. Iz tog razloga se virusi "zakače" na izvršne fajlove legitimnih software-a te na taj način se prilikom pokretanja legitimnog programa učitavaju u radu memoriju i izvršavanju određene radnje za koje su programirani.

Crvi su maliciozni programi koji se mogu replicirati bez intervencije korisnika te se širiti računarskom mrežom kopirajući se na nezaražene računare. Za razliku od virusa crvi se ne kače za legitimne programe već se izvršavaju samostalno. Crvi se najčešće programiraju da bi instalirali "backdoor" (backdoor u računarskom svijetu se odnosi na metode za zaobilaženja legitimnog načina autentikacije na sistem te otvaranje daljinskog pristupa sistemu bez znanja korisnika). Iz ovog razloga crvi su jedna od najvećih prijetnji modernih datacenter-a.

Slika 5: Computer worm, Picasa Google

Trojanski konji se za razlikuju od standardnih malicioznih software-a ne repliciraju samostalno, oni se predstavljaju kao legitimni programi i to najčešće kao antivirusni programi koji uklanjaju određeni virus sa sistema, a u pozadini omogućavaju ulazak drugih virusa na računare kao i otvaranje backdoor-a za nelegalan daljinski pristup računarskim sistemimail podacima. Otuđivanje podataka se najčešće svodi na brojeve kreditnih kartica koje su korištene za plaćanje na internetu, kopiranje povjerljivih fajlova sa računara, ogovanje podataka koji se unose putem tastature (u svrhu pronalaženja lozinki za sisteme) kao i praćenje ekrana korisnika.

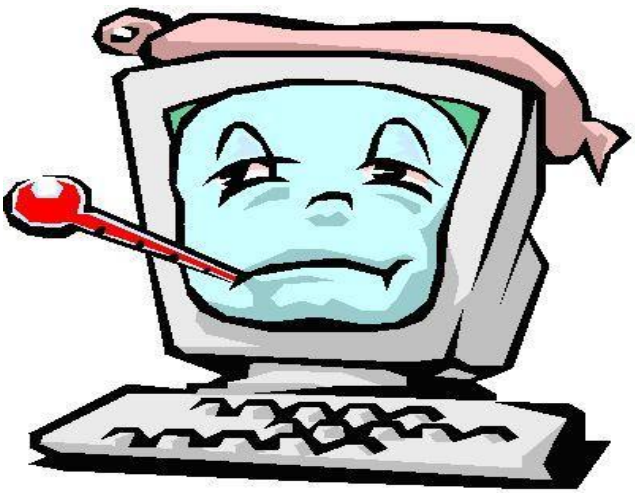
Rootkits su tip nevidljivog malicioznog software-a koji krije postojanje određenih procesa na računaru i omogućava administrativni pristup sistemu. Rootkits iskorištavaju poznate greške u sistemima i aplikacijama za omogućavanje daljinskog pristupa sistemima. Jedan primjer rootkit napada je u Grčkoj u 2004-2005 god. kada je iskorištena greška na mobilnoj mreži Vodafona te je prisluškivano više stotina mobilnih telefona koji su pripadali dužnosnicima vlade Grčke. Za ovaj proboj sigurnosti Vodafon mobilne mreže nikada niko nije odgovarao jer nisu uspjeli otkriti identitet osoba koje su odgovorne za ovaj napad.

Slika 6: Spyware detected, Picasa Google

Spyware su maliciozne aplikacije koje prikupljaju podatke sa računarskih sistema bez znanja korisnika kao što su istorija posjećivanja web stranica kao i djelimičnog preuzimanja kontrole računara u smislu mijenjanja home stranice Internet browser-a, stvaranja nepotrebnog prometa na mreži itd.

Spyware se koriste i za nelegalne reklame koje se aktiviraju na zaraženim sistemima koje su izabrane u skladu sa navikama korisnika prilikom posjete internetu.

Svi mi smo odgovorni za sigurnost računarskih sistema počev od ličnih računara pa do poslovnih datacentara te je potrebno da se svi ponašamo odgovorno prilikom posjete internet stranicama, otvaranja e-mailova od nepoznatih osoba, te instalacije nepoznatih i neprovjerenih aplikacija na računare što može uzrokovati velike štete na poslovnim podacima i sistemima.



Slika 7: Antivirus, Picasa Google