Zbogom Mikelanđelo!

Šesti mart svake godine je loš dan za mnoge vlasnike PC računara - aktivira se po zlu poznati virus Mikelanđelo i obriše deo hard diska na kome se nalaze sve vitalne informacije. Sasvim dovoljno da od diska prepunog podataka ostane gomila sektora koji se obično ne mogu ponovo povezati. Boot virusi su u današnje vreme toliko ozbiljno shvaćeni, da su čak i mnogi proizvođači BIOS-a uveli opciju koja štiti računar od njih. Pošto se radi o pionirskim koracima, bolje rešenje je osloniti se na proveren i pouzdan softver. Predstavljamo dva takva programa.

Kristijan Lazić

U mnogim "velikim" paketima, specijalizovanim za borbu protiv virusa, *boot* infektori nisu baš najslavnije obrađeni. Autori su se najčešće zadovoljavali opcijom koja će *boot* sektor "imunizirati", tj. malo mu promeniti sadržaj, što ponekad (recimo kod zaštićenih disketa) nije prihvatljivo. Ako se *boot* sektor prebriše nekim standardnim i ispravnim, može se desiti da se računar prilikom podizanja sistema ili potpuno blokira, ili da ne funkcioniše pravilno. Nastaje problem koji je doduše redak, ali sigurno i veoma neprijatan kada se pojavi.

Mnogo bolje rešenje je napraviti kopiju čiste particione tabele i *boot* sektora, i naknadno ih samo upoređivati sa originalima. Nemojte žaliti da izgubite pola sata, detaljno proverite sistem, i nabavite jedan ili oba opisana programa. Utoliko pre, jer ćete biti zaštićeni i od tzv. *boot dropper*-a, jedne vrste trojanca ili virusa sa "majčinskom" karakteristikom, koji će u vaš *boot* sektor upisati "padobranca" koji u okviru svoga koda čuva i virus. Naravno, ni razni multipartitni virusi koji neke svoje delove vole da stave u particionu tabelu, neće imati šanse.

INNOC Boot Virus Immunizer

U slučaju da imate pregršt zaraženih disketa, a malo vremena da ih očistite, ovaj mali program je kao stvoren za vas. Pored kratkog i informativnog DOC fajla, u originalnoj arhivi se nalaze i izvršni COM fajl, dugačak samo 178 bajtova, ali i sors programa u asembleru. Jedino na šta treba paziti je da disketa koju ćete imunizirati ne služi za dizanje sistema; pošto se na većinu ipak samo smeštaju podaci, pomenuti uslov ne predstavlja veću prepreku.

INNOC radi na principu preuzimanja kontrole: učitaće *boot* sektor u memoriju, izmeniti par bajtova početka i tako onemogućiti virus da, kojim slučajem, ponovo "oživi", i najzad ga vratiti na disketu. Ako se desi da greškom ubacite neku imuniziranu disketu prilikom podizanja sistema, računar će se samo blokirati, posle čega ga treba resetovati i sistem podići sa neke druge diskete. Naravno, imuniziranje je prelazno rešenje; "vakcinisane" diskete kasnije, po potrebi, možete ponovo osposobiti za podizanje sistema. Velika prednost je u tome što paket sadrži i sors programa, pa ga, ako se razumete u asembler možete doterati po sopstvenoj meri. To je ujedno i osiguranje da program nema neke nedokumentovane ili loše napisane funkcije.

Autor **Mike McCune** je svoje delo stavio u javno vlasništvo, što znači da je korišćenje i posedovanje INNOC-a potpuno besplatno, pa eto razloga više da se arhiva od svega dva kilobajta nađe na vašem disku.

HS

Programi sa kratkim i nezanimljivim nazivima ostaju neprimećeni, što je ponekad prava šteta. Tako se zbilo i u slučaju ovog izvrsnog, i, pre svega, korisnog programa. Autor **Henrik Stroem** je otišao korak dalje od svojih konkurenata, i dobro realizovao problem zaštite tabele particija i *boot* sektora. Ali, krenimo redom.

Program se isporučuje u dva oblika, COM i SYS, koji su funkcionalno potpuno isti. Neznatna prednost je na strani SYS verzije, jer može da se izvrši pre svih ostalih *device driver*-a, i tako prvi proveri sve "kritične" interapte koje *boot* virusi vole da preuzimaju. Pošto ponekad ima problema oko pokretanja HS-a iz CONFIG.SYS-a, COM verzija je ostavljena za AUTOEXEC.BAT, ili eventualno naknadno startovanje iz komandne linije.

Prednosti koje autor navodi u dokumentacionom fajlu su potpuno tačne i proverene u praksi. HS se zapravo jedini izborio sa opasnim **Zharinov** virusom prilikom testa anti-virus programa, i pored *stealth* tehnika koje su virusu omogućavale da zaobiđe sve testirane programe. Ovo će, sigurno, mnogima biti dovoljan razlog da nabave HS, ali i činjenica da nije rezidentan, da zauzima ispod 5 K prostora na disku, i da je potpuno "nečujan", tj. da se javlja tek ako nešto nije u redu, trebala bi da bude dovoljna preporuka. Firme će se za simboličnu cenu zauvek rešiti napasti u vidu *boot* virusa, a svi ostali koji svoj računar koriste za nekomercijalne poslove su slobodni da ga koriste besplatno.

Pošto ste sistem potpuno očistili od virusa, pokrenite HS sa opcijom /M, navedite ime fajla u kome će biti smeštene kopije MBR-a i *boot* sektora, a u CONFIG.SYS ili AUTOEXEC.BAT dodajte odgovarajuću liniju koja će pri svakom podizanju sistema proveravati da li je sve na svom mestu... i zaboravite na Mikelanđela i njegove "rođake". Program će kopiju *boot* sektora i particione tabele snimiti u fajl i ispisati odgovarajuću poruku na ekranu. U slučaju da vam nešto ipak promakne, ili bar mislite da nešto nije u redu, pokrenite HS.COM iz komandne linije i odahnite ili sve prepustite programu - virus će u drugom slučaju automatski biti uklonjen. U slučaju eventualne infekcije, na disku će biti kreiran i fajl HS.INF u kome će biti snimljen izmenjen *boot* sektor, koga kasnije možete na miru analizirati, ili proslediti autoru.

Jedina mana programa je "preosetljivost", koja vam s vremena na vreme može zasmetati. Dakle, ako kojim slučajem promenite operativni sistem, tj. pređete na neku drugu verziju DOS-a, HS će vam u particionu tabelu bez upozorenja vratiti stare

podatke, što može uzrokovati gubljenje podataka na disku. Zato je savet autora ovog teksta, a i autora samog programa da pre svake slične operacije prethodno deinstalirate HS, isključivanjem istog iz CONFIG.SYS, odnosno AUTOEXEC.BAT datoteke. Ako niste baš vični tome, jednostavno obrišite fajl koji HS koristi prilikom provere sistema; program će prijaviti grešku, ali bar neće doći do nepredviđenih situacija. Naravno, situacije poput menjanja operativnog sistema su prilično retke, i bez obzira na (ne)prisustvo HS-a, obavezno napravite *backup* podataka. Za one koje više vole da čuju praktična iskustva, mogu reći da je HS uspešno očistio i niz drugih *boot* virusa, među kojima je, i virus *stoned*, takođe opasan i čest gost mnogih PC-ja.

I par saveta

Ako se držite pomenutih uputstva pri instalaciji INNOC-a i HS-a, svi *boot* virusi će postati prošlost. Sa druge strane, ovi programi vas ne štite od fajl virusa, tako da ćete i dalje morati da proveravate programe koje stavljate na hard disk. Međutim, ni tu situacija nije toliko crna, ali o tome u sledećem nastavku. Naravno, nikad se nemojte potpuno opustiti i poverovati da ste se napasti rešili zauvek. Vremenom će se pojavljivati novi virusi, a možda će neki od njih uspeti da zaobiđu i HS. Ali to je već priča za sebe... i oni će kad-tad biti pobeđeni!

Pošto mnogi virusi programe koji im nisu "po meri" prepoznaju baš po imenu, jedan od saveta je da HS preimenujete: sa novim nazivom se sigurno nećete posle izvesnog vremena zapitati "čemu ovo služi", a neki novi uljezi će biti sprečeni u svojoj nameri. Čak i fajlu koji HS pravi možete dati neko čudno ime i obezbediti se za duži vremenski period. A tada, ko zna... - možda ćemo se Mikelanđela samo sećati!