BOOTPROT v 2.8

Tento program slouží k rychlé antivirové kontrole počítače. Kontroluje neporušenost systémových oblastí počítače, tj. paměti CMOS, hlavní zaváděcí sektor MASTER BOOT, BOOT SECTOR a spustitelné soubory. Pracuje na principu kontrolních součtů a proto dovede odhalit i neznámé (tedy úplně nové viry). Rozeznává jak BOOTviry tak také souborové viry. Všechny bootviry a master bootviry umí také vyléčit. Léčba souborů napadených polymorfním steal virem se nedoporučuje, protože nelze zajistit funkčnost vyléčeného souboru.

Programem BOOTPROT lze taky obnovit funkčnost počítače po napadení virem a nebo pokud dojde k přepsání MBR (master boot record). Byl testován s virem ONEHALF, který napadá jak soubory tak také MBR. Celkem snadno odstranil virus z MBR, soubory se změněnými kontrolními součty může smazat uživatel (klávesou CTRL+D).

INSTALACE

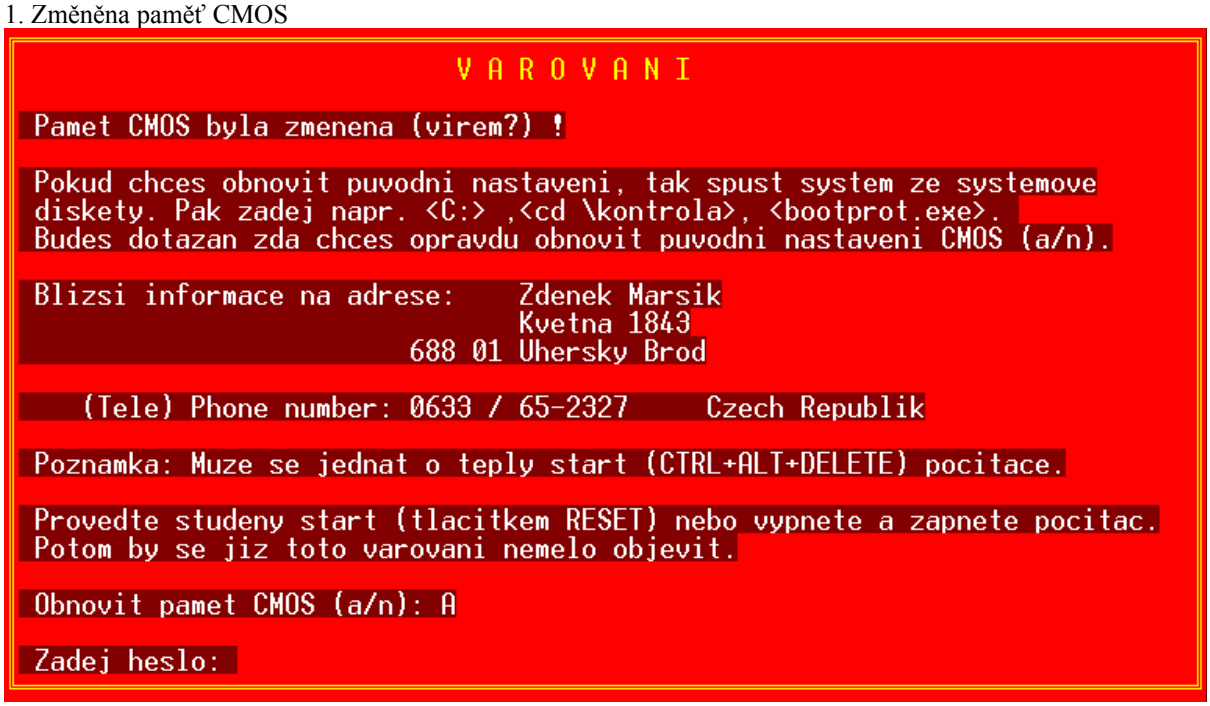
Pro instalaci programu napište INSTALL na instalační disketě. Do AUTOEXECu bude přidán řádek: BOOTPROT C: -3 . Znamená to: Kontroluj paměť CMOS, MASTER BOOT a BOOTSECTOR po každém restartu počítače, pevný disk C: kontroluj každý třetí den na kontrolní součty.

Instalace pro **WINDOWS 95:** Načtěte system z instalační diskety BOOTPROT a spusťte a:\install.exe .

Varovná hlášení

Během probíhající kontroly se může zobrazit jedno z následujících varovných hlášení:

1. Změněna paměť CMOS



Toto hlášení se může objevit po činnosti viru ale stoprocentně objeví po změně konfigurace počítače (například rozšíření paměti RAM z 8 MB na 16 MB).

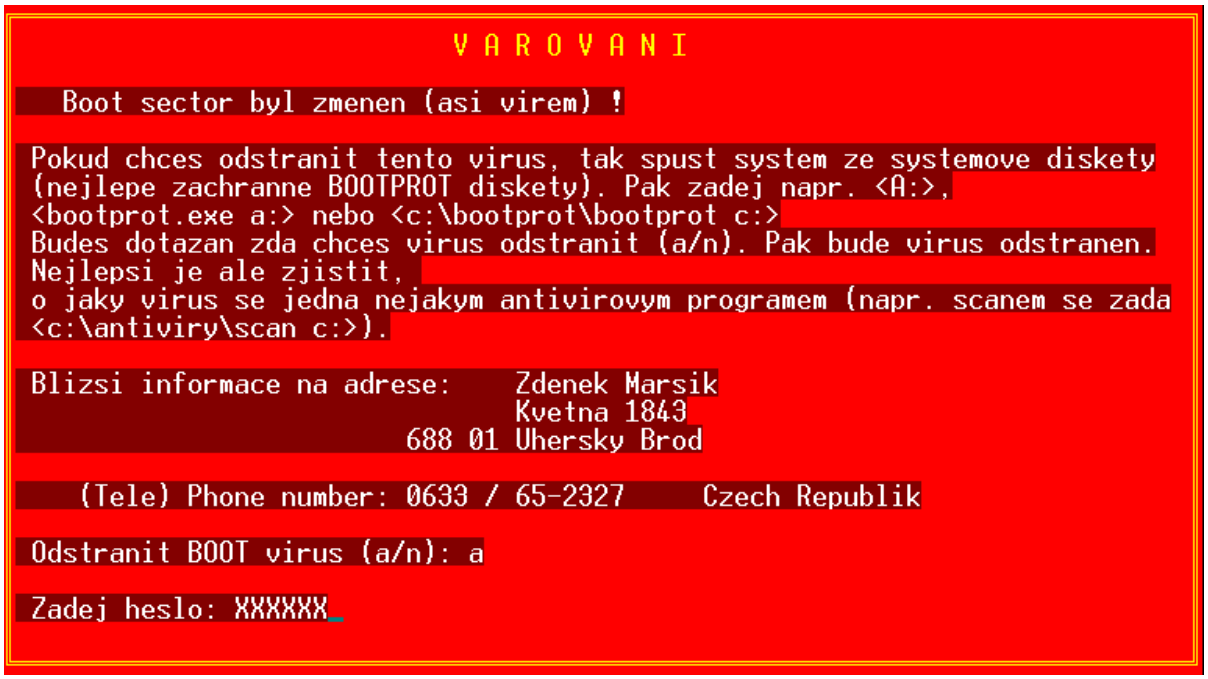
A) Pokud jste měnili konfiguraci počítače, je jasné, že to nebyl virus kdo změnil CMOS. Pak vymažte soubor C:\CMOS.ZAL a proveďte restart počítače.

B) Pokud jste konfiguraci neměnili, došlo ke změně CMOS a můžete ji obnovit po zadání hesla: zabij virus
Taky toto varování můžete ignorovat a stisknout klávesu ENTER .

2. Hlavní zaváděcí sektor (MASTER BOOT) byl změněn

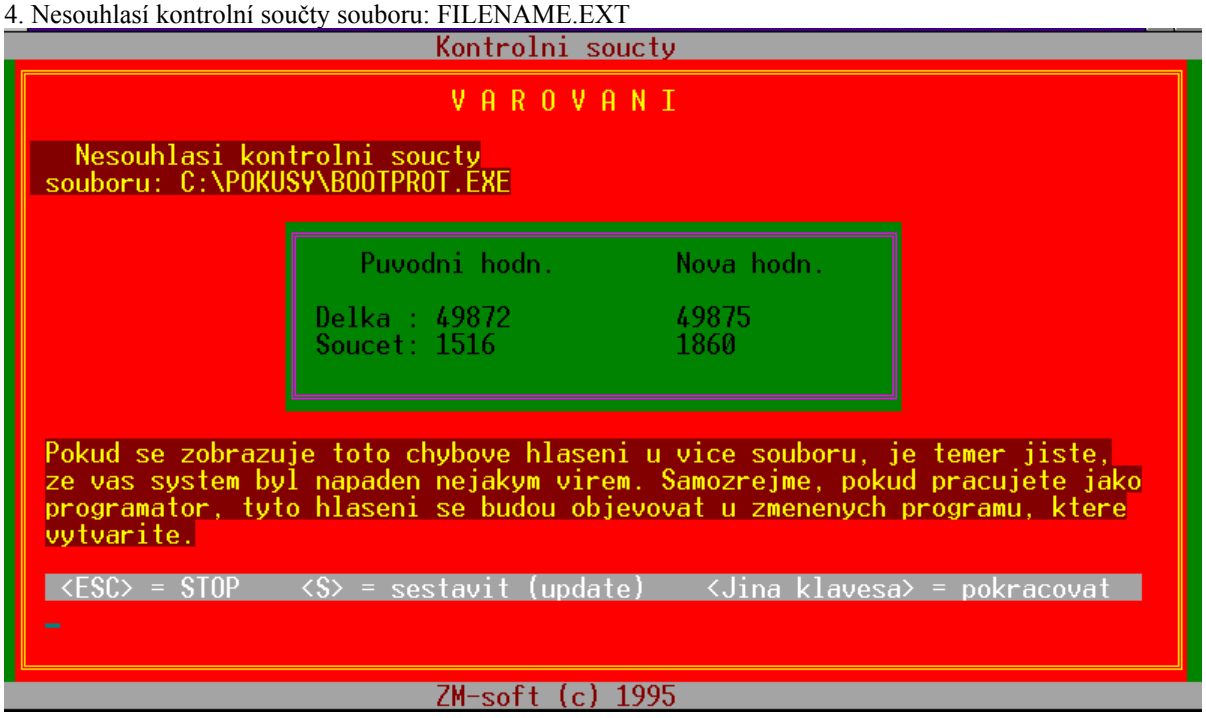
Toto varování je velmi vážné a proto program BOOTPROT zablokuje počítač dokud není virus odstraněn. Pokud jste nenainstalovali nějaký program, který zapisuje do prvního sektoru na pevném disku (což naprostá většina programů nedělá), máte počítač napaden MBR virem (například ONEHALF, česky jedna polovina).
BOOTPROT vás vyzve k vložení systémové diskety (disketa z které jste BOOTPROT instalovali) a k vypnutí počítače. Po zapnutí počítače proběhne načtení operačního systému z diskety. Pokud je disk přístupný, spustí se BOOTPROT a zobrazí se varovné hlášení viz. obrázek 2.
Zadáte *a*, pak heslo *zabij virus* a zobrazí se *virus odstraněn*. Pak už jenom RESET.
Pokud je pevný disk nepřístupný, musíte z této diskety zadat: BOOTPROT A:
MBR bude obnoven a všechna data budou zachována v původním stavu (Například u viru ONEHALF někteří méně znalí formátují pevný disk příkazem FORMAT C: , což zlikviduje Vaše data, ale virus neodstraní).
Taky se nedoporučuje FDISK /MBR, protože výsledek je nejistý.

3. Boot sektor byl změněn (asi virem)



Zde platí vše jako u var. hlášení č. 2.

4. Nesouhlasí kontrolní součty souboru: FILENAME.EXT



Toto varovné hlášení bude u změněných souborů. Nyní je třeba se rozhodnout, kdo to změnil:

1. Já
2. Virus
3. Program se samomodifikuje
4. Upgrade nějakého programu na vyšší verzi (např.: DOOM1 na DOOM2)

Bod 1 připadá v úvahu pouze u programátorů.
Bod 3 je velmi zřídkavý.

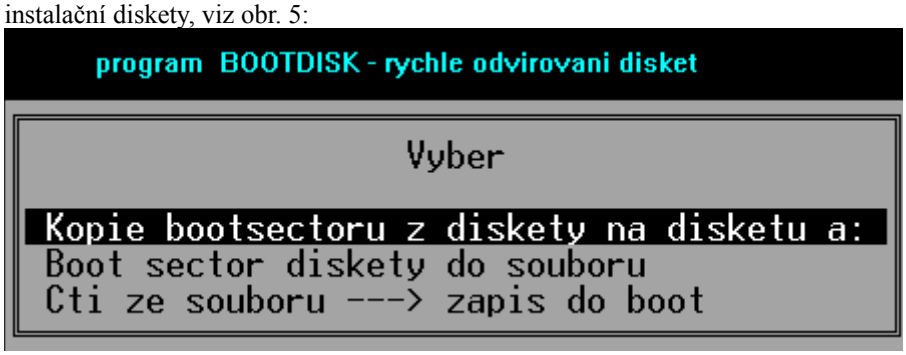
Bod 2 napadení souborovým virem

U varovného hlášení č. 4 je vždy napsáno jméno podezřelého souboru, původní délka souboru a původní hodnota kontrolního součtu hlavičky. Nyní můžeme stisknout STOP pro přerušení programu, SESTAVIT (update) pro aktualizování kontrolního součtu nebo pokračovat (jiná klávesa). Pokud jste provedli upgrade nějakého programu (např.: t602 v 3.0 na verzi 3.1) stiskněte klávesu *s* pro znovusestavení kontrolního součtu. Pokud nejde o upgrade a nepracujete jako programátor, jde s velkou pravděpodobností o virus (zvláště zobrazuje-li se toto hlášení u více souborů). Pak stiskejte např. mezerník, je-li toho moc tak *ESC*. V souboru C:\KONSOUC.TXT je zaznamenáno jméno souboru a délka předpokládaného viru. Pokud je například změněno 30 souborů a předpokládaná délka viru je vždy stejná (např. 1376 bytů), pak jste nakaženi virem (1376=HELLOWEEN 1376). Doporučuji si potom vytisknout soubor *konsouc.txt* , pak zasunout instalační disketu BOOTPROT a vypnout počítač (bez napájení umře každý virus v paměti). Po zapnutí počítače začne probíhat kontrola (pokud ne tak ji spusťte příkazem *a:\bootprot a: -0*) a jsou vypisována varovná hlášení. Mačkejte kombinaci kláves *CTRL+D* pro vymazání viru (i se souborem). Taky se můžete pokusit léčit napadené soubory jiným antivirovým programem. Toto ovšem antivirové firmy nedoporučují a je lépe napadené soubory smazat a znovu nainstalovat.
Jsou také viry, které předstírají původní velikosti souborů (např. TREMOR). Proto nejjistější kontrola je tato:
1. Vypnout napájení počítače
2. Vložit instalační disketu BOOTPROT v 2.7
3. Zapnout napájení počítače

U takto provedené kontroly je zcela bezmocný i TREMOR (a každý jiný virus).

Odvirování disket napadených BOOT virem

Na instalační disketě je program BOOTDISK.EXE, který slouží k rychlému odvirování velkého počtu disket. Po virové nákaze BOOT nebo MBRBOOT virem jsou také napadeny bootsectory všech vašich disket (přesněji disket s kterými jste pracovali po dobu nákazy). Pro odvirování disket spusťte program BOOTDISK.EXE z instalační diskety, viz obr. 5:



Volbou *Kopie bootsectoru z diskety na disketu a:* dojde k velmi rychlému odvirování diskety (asi 3 vteřiny, u antivirového programu AVG je to asi 30 vteřin a pouze u virů které zná).

Odinstalování programu BOOTPROT

Pokud se rozhodnete prodat svůj počítač (nebo pouze pevný disk) musíte program BOOTPROT odinstalovat z instalační diskety příkazem *uninstal*. Provede se odinstalování programu včetně kontrolních součtů a program BOOTPROT můžete znovu instalovat (např. na Vašem novém počítači).
Také doporučuji použít uninstal po upgradu vašeho hardwaru. Je to jednoduché, zadáte z instalační diskety *uninstal* a potom *install*.
Programem SMAZEJ.EXE lze vymazat všechny kontrolní součty. Po restartu počítače budou znovu vytvořeny.

Příjemnou práci s programem a virům zmar přeje: Autor: Zdeněk Maršík

Květná 1843

688 01 Uherský Brod