M2- Securitatea sistemelor de calcul și a rețelelor de calculatoare

Lecția 1: Aplicații malefice-mod de răspândire, efecte

Clasa a-XII- a A

Un **virus** este un program software de dimensiuni mici care se răspândește de la un computer la altul și interferează cu funcționarea computerului. Un virus de computer poate să altereze sau să șteargă date de pe un computer, să utilizeze un program de e-mail pentru a răspândi virusul pe alte computere sau chiar să șteargă tot conținutul unui hard disk.

Un **vierme** este un cod de computer care se răspândește fără interacțiune cu utilizatorul. Majoritatea viermilor încep ca atașări de e-mail care, atunci când sunt deschise, infectează computerul.

Un **cal troian** este un program software rău intenționat care se ascunde în alte programe. El plasează în sistemul de operare un cod care permite hackerului să acceseze computerul infectat. De obicei, caii troieni nu se răspândesc singuri. Ei sunt răspândiți de viruși, de viermi și de software-uri descărcate.

Spyware-urile se pot instala pe computer fără cunoștința dvs. Aceste programe pot să modifice configurația computerului sau să colecteze date publicitare și informații personale. Programele spyware pot urmări obiceiurile de căutare pe Internet și, de asemenea, pot redirecționa browserul dvs. web către alt site web decât cel pe care doriți să îl accesați.

Un **software de securitate răuvoitor** încearcă să vă convingă că aveți computerul infectat de un virus și, de obicei, vă solicită să descărcați sau să cumpărați un produs care elimină virusul. Software-urile de securitate răuvoitoare pot împiedica deschiderea unor aplicații sau pot afișa fișiere Windows legitime și importante ca infecții.

Malware este un termen utilizat pentru desemnarea software-urilor rău intenționate concepute să provoace daune sau să efectueze acțiuni nedorite în sistemul unui computer. Exemple de malware:

- Viruși
- Viermi
- Cai troieni
- Spyware
- Software-uri de securitate răuvoitoare

Google a indentificat 150 de aplicatii in Play Store ce puteau fura datele personale ale utilizatorilor, inclusiv datele bancare. Aplicațiile nu afectau sistemul Android, însă puteau infesta rapid calculatorul utilizatorilor,atunci când aceştia îşi conectau telefonul afectat la Windows. Majoritatea aplicațiilor învățau utilizatorii diverse abilități, de la cusut până la repararea unei biciclete. Atunci când era transferat accidental din telefon în calculator, fișierul **keylogger** era ascuns sub denumiri precum 'Android.exe', 'my music.exe,' 'COPY_DOKKEP.exe,' 'js.exe,' 'gallery.exe,' 'images.exe,' 'msn.exe' si 'css.exe' (exemple de astfel de aplicații: Baby Room, Tattoo Name, Car garage, Yoga Meditation, Mens Shoes).

Lecția 2: Aplicații de securitate

Eliminarea unui virus de computer sau a unui spyware poate fi dificilă fără ajutorul unor instrumente de eliminare a software-urilor rău intenționate. Unii viruşi de computer şi alte software-uri rău intenționate se reinstalează după detectarea și eliminarea virușilor și a programelor spyware. Există o serie de aplicații de securitate oferite de companii precum Microsoft și care odată instalate pot elimina aplicații malware ce ne infestează calculatorul.

Aplicațiile de securitate sunt instrumente cu rol în detectarea şi eliminarea virușilor. Cele mai importante module ale sistemelor de securitate sunt cele de scanare, diagnosticare şi protejare împotriva programelor de tip spion, viruși, cai troieni sau multe altele.

În afara **programelor antivirus** cunoscute de orice utilizator, **Microsoft** (dau ca exemplu această companie pentru că ea este cea care oferă familia de SO Windows pe care și noi o folosim) oferă gratuit o serie de recomandări și instrumente de înlăturare a aplicațiilor malware. De exemplu:

Microsoft Safety Scanner sau **Malicious Software Removal Tool** -instrumente online gratuite care scanează și ajută la eliminarea potențialelor amenințări din computer.

Recomandări:

-actualizarea permanentă a computerului (SO, aplicații software, mai ales, program antivirus);

-activarea firewall-ului (paravan de protecție-instrument oferit de Microsoft la instalarea SO);

-Instalarea programelor **Microsoft Security Essentials** sau A**ntivirus Windows Defender** și actualizarea lor permanentă.

Foarte utile în protecția calculatorului sunt și programele de curățat calculatorul (dar nu suficiente). Acestea sunt realizate pentru ștergerea fișierelor temporare sau nedorite lăsate de anumite programe, eliminarea istoricului de navigare, cookie-uri și cache, curățarea, optimizarea și corectarea regiștrilor de Windows, dezinstalarea de programe, eliminarea fișierelor rămase după dezinstalarea unui program. Însă unele astfel de programe au și o funcție care permite **detectarea și eliminarea de viruși.** Un program de curățare foarte cunoscut și eficient, gratuit este **CCleaner.**

Cum le putem folosi?

Foarte simplu. Trebuie doar să le descărcăm și instalăm pe calculator. Apoi să folosim funcțiile ce le oferă programul prin deschiderea meniului și selectarea funcției dorite.

Cum se instalează un program antivirus sau un program de curățare? Ca orice aplicație software. După descărcarea programului, se urmează pașii instalări în ordinea în care apar.

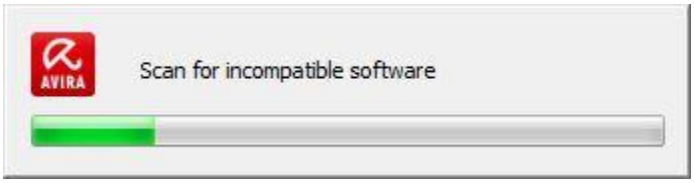
Observație: Instalarea unui **program antivirus** nu este suficientă pentru protecția sigură a calculatorului. Un program antivirus nu poate proteja calculatorul de toate aplicațiile malware existente. Fiecare program antivirus poate proteja calculatorul de anumite aplicații malware. În funcție de nevoile noastre trebuie să ne alegem programul antivirus cel mai potrivit. De exemplu: **Kasperski,** program antivirus cunoscut este cel mai bun pentru cumpărături și servicii bancare online. **Bitdefender Securitate Totală-**oferă o serie de funcții suplimentareși oferă o securitate online foarte bună.

Notă:

Chiar dacă toți știm să instalăm un program antivirus, aveți ca exemplu instalarea programului antivirus Avira (gratis pe Internet dar deloc, fantastic)

Instalare Avira

1. Descărcăm Avira Free Antivirus și îl deschidem

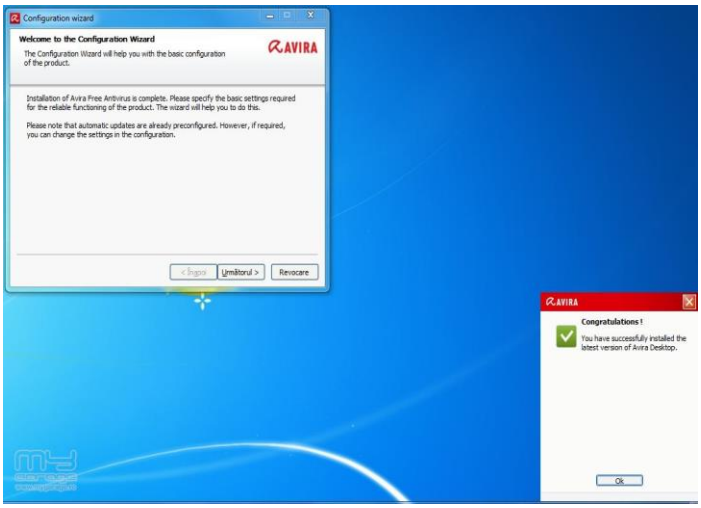


2. În fereastra **choose installation type**, selectăm **Custom** si bifăm **i accept the E.U.L.A**

3.Aici debifăm tot pentru a nu instala toolbar-ul

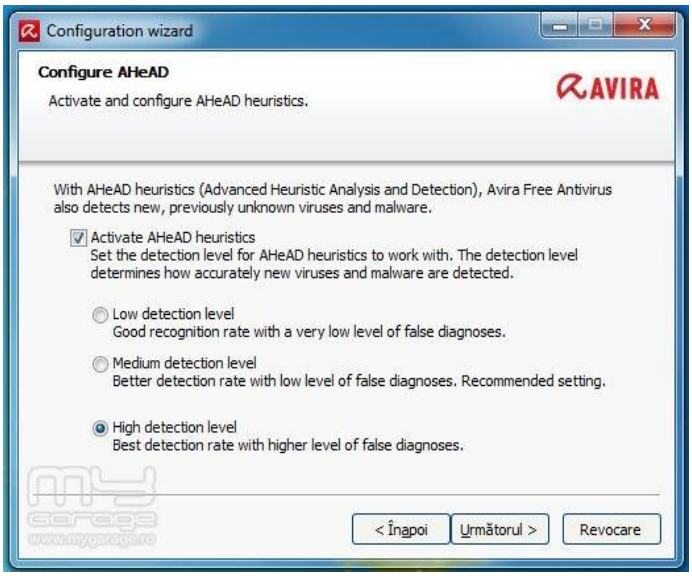
4. In ferestrele următoare ne întreabă în ce dosar să instalăm Avira, ce componente să instalăm şi locul unde sa apară scurtăturile programului.
(notă: de preferat este să nu modificăm nimic aici)

5. După ce programul a fost instalat, trebuie să ne apară doua ferestre ca în poza de mai jos

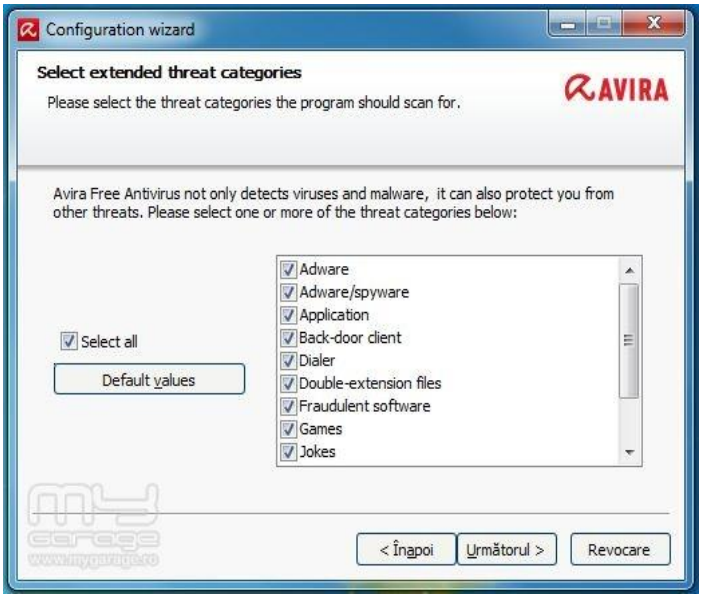


6. Aici în fereastra **Welcome to the configuration wizard**, facem click pe butonul: **următorul**

7. În fereastra **Configure AHeAd**, bifam **High detection level**



8. Aici bifăm **select all**



9. Iar în fereastra **Realtime protection start mode** bifăm **Secure start**

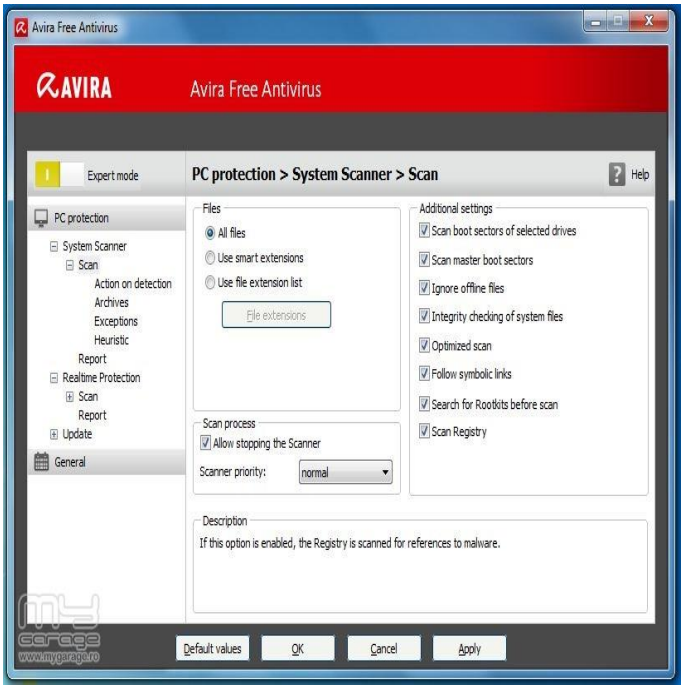
10. În ultima fereastră ne întreabă dacă dorim să scanăm sistemul după ce închidem configuratorul.

Configurare Avira

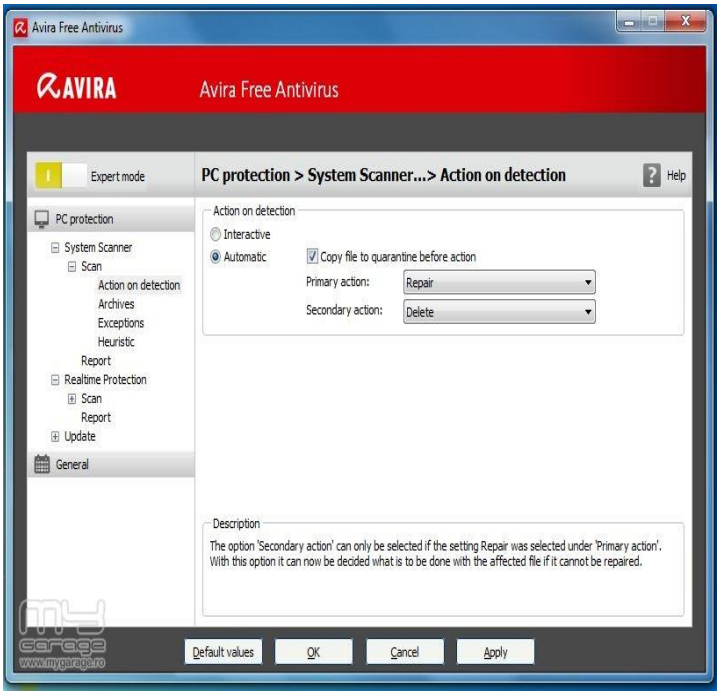
1.Deschidem programul și sus în tabul **Extras**, facem click pe **configuration**

2.Aici facem click pe **expert mode** și la mesajul de avertizare selectam **yes/da**

3. Aici la **Pc Protection - System Scanner - Scan** bifăm **all files** și tot din dreapta la **additional settings**



4. În ramura **action on detection,** selectăm **automatic,** bifam **copy file to quarantine before action** şi la **Primary action** selectăm **Repair** iar la **Secondary action** selectăm **Delete**



5. În ramura **Archives** bifăm **All archives types.**

6. La Realtime Protection bifam **All files** si la **Archives** bifăm **Scan archives** unde aici introducem valoarea **10** la **Max. recursion depth.**