

PROTECȚIE MAXIMĂ!

Pericolul virușilor crește considerabil din cauza noilor tipuri de atacuri, dar și din cauza vulnerabilităților sistemelor de operare și ale sistemelor de securitate.

Lupta virtuală dintre viruși și calculatorul tău pare să țină la nesfârșit și nu va exista un câștigător detașat, oricâte filme în genul Matrix se vor face. Ingeniozitatea hackerilor și a celor care creează viruși au făcut ca „tranșeele” luptei să se mute la toate dimensiunile virtuale cunoscute: deja clasicele CD-uri și DVD-uri, stickuri de memorie, rețea, Internet (torrente, programe P2P, site-uri false, programe de chat, etc.).



Armele „atacurilor” rămân aceleași: troieni, spyware, boți¹, rootkituri², keylogger³, însă ele sunt îmbunătățite permanent și, de aceea, producătorii pachetelor de antivirusi investesc timp și resurse pentru a fi la curent cu toate pericolele apărute. Iar asta pentru că există o luptă și la nivelul „apărătorilor” pentru a deveni cel mai bun antivirus. Locul 1 se schimbă foarte des, însă competiția producătorilor de securitate nu poate fi decât un motiv de bucurie pentru noi, utilizatorii.

În acest sens, mi-am propus în continuare să vă prezint un punct de vedere personal, referitor la aceste competiții, și în același timp să vă ofer câteva sfaturi pentru a vă proteja eficient împotriva virușilor, răspunzând pe scurt la următoarele întrebări:

1. Care sunt pericolele pentru calculator?
2. Cum te protejează programele antivirus?

1. Care sunt pericolele pentru calculator?

- **Virusii:** clasicii viruși care au infectat fișierele obișnuite (documente, aplicații) de când există calculatoarele. De ordinul miilor, aceștia pândesc parcă orice oportunitate de a se descărca pe hard diskul tău pentru a infecta cât mai multe fișiere. Ținta lor nu s-a schimbat prea mult, cele mai frecvente sunt documentele Excel și executabilele programelor.
- **Worm:** În traducere liberă, viermi, acest tip de fișiere atacă folosind calea Internetului și, de cele mai multe ori, se află în e-mailuri contaminate având ca scop răspândirea prin mesaje de tip mass⁴. Pericolul lor nu este

¹ **Boți:** programe automatizate ce pot găsi pe adrese de Internet bucăți de text sau diverse informații. Aflat pe un calculator, un bot poate trimite unui site, de exemplu, toate adresele de Internet vizitate de către un utilizator.

² **Rootkit:** tip de virus foarte periculos ce reușește să treacă de multe ori nedetectat de sistemele de securitate instalate pe un calculator. Un rootkit imită fișiere ale sistemului de operare și poate camufla și alte tipuri de viruși.

³ **Keylogger:** fișiere malițioase ce înregistrează intrările de la tastatură, salvând astfel parole și nume de conturi, informații bancare, etc.

⁴ **Mesaje mass:** e-mailuri ce conțin ca atașamente diferite fișiere ce sunt trimise unor anumite persoane și sunt trimise mai departe apropiaților de cele mai multe ori datorită mesajului atractiv. Atașamentele mesajelor pot fi infectate cu viruși.

foarte ridicat și de cele mai multe ori un antivirus actualizat îl identifică imediat sau sunt trimiși la coșul de gunoi de către filtrele antispam⁵.

- **Rootkit** : Printre cele mai noi pericole apărute, acestea sunt create având o tehnologie de „invizibilitate” ridicată față de sistemele de detecție. Camuflarea are loc prin modificarea fișierelor din Windows pentru a evita scanările antivirusilor. Problema este cu atât mai gravă cu cât rootkiturile reușesc să ascundă și alte tipuri de fișiere malițioase pentru a putea infecta în totalitate calculatorul dumneavoastră.
- **Troieni**: Aceste fișiere sunt ascunse în kiturile de instalare ale programelor gratuite descărcate de pe Internet. Pericolul este mai evident când programul descărcat este făcut de o anumită persoană și nu de către o companie software. Troienii identifică datele personale pe care le folosești pe Internet și le înregistrează pentru a le trimite pe ascuns celui care ți-a trimis fișierul infectat. Un alt tip de Troieni sunt boții, fișiere cu ajutorul cărora cineva din exterior poate controla calculatorul dumneavoastră infectat.
- **Drive-by-downloads**: Din nou o cale de infiltrare recent apărută care are ca scop descărcarea troienilor sau a altor tipuri de fișiere pe calculator, și asta doar prin vizitarea unor adrese de Internet. Cei care navighează pe astfel de site-uri periculoase nu trebuie decât să facă clic pe un anumit link sau să își aducă adresa de e-mail în baza de date a site-ului. Virușii ajung ulterior pe hard disk din cauza vulnerabilităților browserelor⁶. Astfel în loc să trimiți o felicitare unui prieten pe calea Internetului, de fapt îi poți trimite un virus care să se infiltreze în calculatorul său în cazul în care e-mailul este deschis. De asemenea, deschiderea unor linkuri aparent inofensive te pot redirecționa către adrese de Internet pline de pericole.

2. Cum te protejează programele antivirus?

Modulele de scanare ale antivirusilor diferă de la versiune la versiune și mai ales de la producător la producător. Pentru că nu mi-am propus să fac gratuit reclamă unui astfel de producător, consider util să discutăm despre principalele metode de detectare a virușilor: proceduri clasice (identificarea semnăturilor de viruși și scanările euristice) și proceduri noi (recunoașterea comportamentală a virușilor).



a. Identificarea semnăturilor de viruși: este cea mai sigură metodă pentru detectarea și eliminarea virușilor, dar și cea mai laborioasă în același timp. Experții de la companiile ce produc antivirusi analizează fiecare fișier malițios descoperit și îi creează o anumită descriere pentru a-l putea încadra într-o categorie anume. Programele antivirus primesc periodic aceste descrieri prin funcția de update și le compară cu fișierele scanate pe hard disk sau cu cele cu care intri în contact direct pe Internet.

b. Scanările euristice: analizarea codului programului scanat de către antivirus. Structura codului, precum și modul în care acesta a fost creat, pot da indicii foarte clare dacă un fișier este sau nu un virus. Această căutare se face în funcție de caracteristici mai puțin clare ale virușilor. Deși este mai rapidă, căutarea euristică nu este la fel de eficientă ca identificarea semnăturilor de viruși.

c. Recunoașterea comportamentală: una dintre cele mai noi soluții de identificare a virușilor, care acționează ca un câine dresat să recunoască anumite mirosuri. Practic, este vorba despre identificarea pașilor făcuți de către viruși pentru a se camufla sau pentru a infecta calculatorul și blocarea acestor pași în momentul în care

⁵ **Filtru antispam:** modul de securitate aflat în majoritatea pachetelor antivirus ce scanează e-mailurile primite pentru a evita mesajele ce conțin atașamente infectate sau pentru a bloca e-mailuri reclamă.

⁶ **Vulnerabilități browser:** breșe existente în codul sursă al browserului ce sunt exploatate de către viruși, iar utilizatorul poate descărca fără să știe anumite fișiere sau să navigheze adrese de Internet nesigure, fără ca antivirusul să realizeze acest lucru la timp.

sunt făcuți, fără a fi descoperiți virușii propriu-zisi. Succesul acestei metode nu este unul deplin, randamentul fiind unul mediu.

Studiile online arată faptul că numărul virușilor crește agravant de la an la an, astfel încât în fiecare zi sunt descoperite peste 15.000 de noi pericole. Nu-i de mirare că industria antivirușilor trebuie să facă eforturi pentru a ține pasul, fiind astfel create noi tehnologii pentru depistarea virușilor. Pentru a atrage utilizatorii, acestea au nume speciale: „Sonar” sau „Deep Scan”, însă numele nu este întotdeauna destul.

FLUERAȘ FLORINEL

Șef Birou Comunicații și Informatică

Bibliografie:

- Revista COMPUTERBILD ROMÂNIA, NR.4, Aprilie 2008
- www.computerbild.ro