Viruşii informatici pe înţelesul tuturor

Ce este un virus? În lumea vie, un virus este o entitate biologică de un tip aparte: incapabil să se reproducă numai prin mijloace proprii, el pătrunde într-o celulă, îşi inserează materialul genetic în cel al celulei-gazdă şi foloseşte programele genetice ale acesteia pentru a se multiplica. Deşi cercetări recente au arătat că nu toate virusurile sunt dăunătoare, ba unele chiar pot avea roluri benefice pentru gazdă, percepţia comună asociază virusurile cu răul, cu boala. Această asociere a inspirat şi denumirea dată unor programe de computer capabile de a face rău: **viruşi informatici**.

Două lămuriri:

1. În biologie se foloseşte, drept plural, termenul "virusuri", în timp ce în informatică, ne-am obişnuit în asemenea măsură să le zicem "viruşi", încât aşa le-a rămas numele.
2. Viruşii informatici reprezintă doar una dintre categoriile de programe vătămătoare - aşa-numitele **malware** - ce pot infecta computerele. Viruşii reprezintă, într-un fel, copilăria fenomenului malware; azi, ameninţări mai sofisticate şi mai diversificate au complicat enorm problema protecţiei computerelor. Aşa-numitele programe anti-virus realizate azi sunt, în realitate, programe anti-malware capabile să detecteze şi să elimine o gamă largă de ameninţări, de diverse tipuri. Dar, în accepţia comună a termenului, sunt numite *viruşi* fel de fel de programe dăunătoare care infectează la un moment dat computerul.

Vom trece în revistă - pe scurt principalele categorii de malware ce ne ameninţă computerele şi reţelele şi să amintim câteva dintre cele mai periculoase şi răufăcătoare astfel de programe, care au produs pagube şi panică în lumea utilizatorilor, de-a lungul timpului.

Un **virus**, în înţelesul strict al termenului, este un program care, odată pătruns în computer, se ataşează, în general, de fişiere executabile; când acestea sunt deschise, virusul se răspândeşte şi la alte asemenea fişiere. Deşi există şi unii viruşi creaţi doar ca să se răspândească, pur şi simplu, fără alte consecinţe, aproape întotdeauna viruşii poartă şi instrucţiuni menite să modifice (în general deteriorându-le) fişierele din computerul infectat.

Worm ("vierme") este un program capabil să se răspândească în mod autonom, fără a fi necesar să se atașeze de alte programe din computer. Ca și virușii, programele de tip worm creează probleme, fie măcar prin faptul că consumă din lărgimea de bandă necesară transmiterii de date, încetinind traficul. Dar, de cele mai multe ori, fac mult mai mult rău decât atât.

Troian (de la "cal troian" - Trojan horse sau trojan) este un program dăunător deghizat într-unul pașnic sau chiar dezirabil. (Știți povestea calului troian, din mitologia greacă: în timpul războiului cu Troia, grecii, la sfatul lui Ulise, au construit un uriaș cal de lemn, pe care l-au lăsat în fața Troiei; fără să se gândească prea mult, locuitorii acesteia, încântați, l-au dus în cetate; la căderea nopții, din burta calului au ieșit războinicii greci, care i-au măcelărit pe toți cei din oraș și astfel a fost cucerită Troia.)

Un troian se prezintă ca un fișier inofensiv și interesant, tentându-l astfel pe utilizator să îl descarce de pe Internet, după care, precum grecii înarmați din burta calului, iese la iveală pericolul: software-ul malefic poate șterge documente sau poate instala alte programe vătămătoare.

Un troian, un worm sau un alt tip de malware poate fi utilizat pentru a instala un sistem de acces fraudulos, **backdoor** ("ușa din dos", cum ar veni), care permite unor operatori rău-intenționați să se strecoare în sistem eludând procedurile de autentificare. Așa reușesc hackerii să pătrundă în computere, trecând de barierele de siguranță care îi opresc pe alți utilizatori.

Rootkits sunt tehnici folosite pentru a ascunde faptul că au fost instalate anumite programe nedorite; în cadrul unor asemenea operațiuni, este modificat sistemul de operare al computerului-gazdă, astfel încât programul malware să fie disimulat, ferit de sistemele de detecție. Uneori, asemenea tipuri de malware conțin instrucțiuni care nu numai că le fac aproape de nedetectat, dar împiedică și ștergerea lor.

Spyware este un tip de malware care, instalat pe un computer fără știrea utilizatorului și greu de detectat, adună informații despre acesta și le face accesibile altor persoane, care utilizează aceste informații în propriul lor interes. Un program spyware poate afla fel de fel de date: ce fel de site-uri web vizitează adesea utilizatorul, dar și date de logare pe diverse site-uri, informații legate de finanțele personale și altele, care, ajunse în mâinile cui nu trebuie, pot genera probleme. Uneori, e vorba doar de bombardamente plictisitoare și enervante cu mesaje publicitare bine țintite; alteori, însă, e vorba despre lucruri mai grave, precum aflarea numărului cărții de credit (urmată de golirea contului).

Programele malware evoluează continuu, devenind din ce în ce mai sofisticate, mai greu de detectat și de înlăturat; în același ritm, se dezvoltă sistemele de protecție, menite să apere computerele de intruziuni și atacuri. E un fel de "cursă a înarmărilor", dramatică și cu mize importante într-o lume modelată și dominată în mare măsură de computere și de Internet.

Și, pentru a ilustra vulnerabilitatea lumii informatice și necesitatea utilizării celor mai bune protecții pe care ni le putem permite, iată câteva dintre evenimentele istoriei scurte, dar intense ale războiului cu malware-ul.

ILOVEYOU a fost un worm care, pornind din Filipine, a infectat inițial computerele prin e-mail. Prezentându-se sub forma unei "scrisori de dragoste de la un admirator secret/o admiratoare secretă" (vă dați seama cum s-au grăbit oamenii să deschidă un asemenea mesaj!), e-mail-ul purta un atașament care, odată deschis, a produs mari necazuri."Virusul" (să-i zicem și noi așa, pentru ușurința comunicării, chiar dacă am explicat mai sus diferența dintre virus și worm și faptul că nu orice malware este, strict vorbind, un virus) se autocopia și ascundea copiile în diverse fișiere din computerul victimei; înlocuia diferite fișiere cu copii ale sale; se transmitea singur prin e-mail, descărca singur de pe Internet o aplicație

capabilă să "fure" parole de computer şi să le transmită celui care crease virusul.La vremea respectivă, în Filipine nu existau legi care să pedepsească infracţiunile informatice, aşa că, deşi a fost cercetat un anume Onel de Guzman, bănuit a fi creatorul virusului, el a fost achitat din lipsă de probe. Conform unor estimări, virusul ILOVEYOU ar fi produs pagube de cca. 10 miliarde USD.

Melissa, creat de americanul David L. Smith în 1999, a fost unul dintre primii viruşi care a atras atenţia publicului. Melissa era un virus care se răspîndea prin e-mail; odată activat (prin deschiderea mesajului infectat), virusul se autoreplica şi era transmis la alte 50 de persoane din lista de contacte a utilizatorului. Virusul a provocat o asemenea aglomerare a traficului de e-mail, încât unele companii au fost silite să sisteze trimiterea de mesaje e-mail pînă la îndepărtarea virusului.

Klez a reprezentat un jalon important în istoria viruşilor informatici. A apărut în 2001 şi, timp de mai multe luni, a afectat Internetul în moduri foarte neplăcute pentru utilizatori. Una dintre caracteristicile fenomenului Klez a fost faptul că, pornind de la tipul de bază, hackerii au modificat virusul, la puţin timp după apariţia sa pe net, creând versiuni diferite, dintre care unele erau deosebit de nocive. În funcţie de variantă, Klez putea acţiona ca un virus obişnuit, ca un worm sau ca un troian; unele variante puteau dezactiva sistemul anti-virus al computerului, iar altele puteau face computerul infectat pur şi simplu inutilizabil. Altele provocau blocarea inbox-ului din cauza numărului uriaş de mesaje sosite într-un timp foarte scurt, ca urmare a faptului că erau programate să trimită masiv "spam"-uri, câteodată de pe adresa, însuşită fraudulos, a unui contact real din lista de adrese a utilizatorului. Una peste alta, a fost un malware care a creat probleme, cu atât mai neplăcute, cu cât numărul mare de versiuni, cu proprietăţi diferite, făcea foarte dificilă studierea lui şi găsirea unor căi de combatere.

Code Red şi **Code Red II**, apărute în 2001, exploatau vulnerabilităţile sistemelor de operare ale computerelor ce rulau Windows 2000 şi Windows NT.În special Windows 2000 s-a dovedit sensibil; într-un computer cu acest sistem de operare şi care fusese infectat, Code Red II crea o breşă (backdoor-vezi mai sus) care permitea unui cracker să acceseze şi să controleze computerul, putând chiar să-l utilizeze pentru a comite infracţiuni. Victima - utilizatorul obişnuit al computerului - nu numai că avea de-a face cu un computer care nu mai mergea cum trebuie, dar ar fi putut fi şi acuzată de delicte, în vreme ce adevăratul vinovat - crackerul care introdusese virusul - rămânea ascuns şi necunoscut.

Nimda (2001) a fost un worm destinat să infecteze serverele, încetinind considerabil traficul pe internet. Una dintre caracteristicile sale cele mai frapante a fost viteza foarte mare cu care se răspândea, iar faptul că infecta serverele a determinat colapsul unor reţele de computere.

SQL Slammer/Sapphire, un virus al serverelor, a provocat, în 2003, pagube estimate la 1 miliard USD; a fost vorba despre evenimente precum căderea serviciului de bancomat al Bank of America, probleme cu serviciul de apeluri de urgenţă 911 în Seattle, erori în sistemul de emitere a biletelor de avion electronice şi, în consecinţă, anularea unor zboruri - efecte care arată cât de grave pot fi urmările unui atac de malware în lumea contemporană, masiv informatizată.

Storm Worm (cunoscut şi sub numele de Nuwar) a debutat în 2006; este un troian care permite controlul de la distanţă al computerelor de către crackeri, care le folosesc, de pildă, transformându-le în "fabrici de spam". A cam speriat lumea internetului prin amploarea atacului dar, deşi cu o răspândire foarte largă, s-a dovedit, din fericire, relativ uşor de îndepărtat, cu ajutorul unor programe anti-virus obişnuite.

Alte atacuri nu sunt însă la fel de uşor de înfruntat, ci necesită soluţii mai sofisticate, mai ales că fenomenul malware a trecut de la computerele de birou şi servere la tot mai multe dispozitive electronice,

putând afecta, cu consecinţe încă greu de evaluat, fel de fel de aparate, de la MP3 playere la smartphone-uri şi cine ştie câte altele.

Informatician Mara Alexandra IVAN

Casa Corpului Didactic Tulcea