INTERNETUL și „răufăcătorii" lui

În primele șase luni ale lui 2008, utilizatorii de Internet au fost nevoiți să facă față zilnic la aproximativ 2.000 de noi viruși sau mutații ale acestora, la 50.000 de atacuri de phishing pe lună și la peste 1.000.000 de calculatoare compromise, ce răspândesc bots sau rootkits, troieni sau alte forme de malware. În al doilea semestru din 2008, distribuția de malware prin intermediul site-urilor infectate a crescut din nou, de aproape 5 ori.

Autorii de malware și-au concentrat atenția asupra producerii și distribuției de troieni, dar și în direcția exploatării vulnerabilităților de sistem, acestea din urmă constituind o problemă din ce în ce mai stringentă, care se prevede a continua să se facă simțită și în 2009.

Unul dintre ultimele atacuri informatice la scară largă identificat de specialiștii BitDefender în 2008 a vizat furtul parolelor de acces. Deghizat într-un plug-in al browserului Mozilla® Firefox®, Trojan.PWS.ChromeInject.A sustrăgea datele de identificare trimise de utilizator către mai mult de 100 de site-uri de e-banking și e-commerce.

Trendul continuă să se facă simțit, iar 2009 a și început cu o epidemie virală de proporții serioase, bazată și ea pe exploatarea unor vulnerabilități în sistemele de operare Windows. Virusul Downadup (cunoscut și sub numele de Conficker sau Kido și detectat în prima sa variantă la sfârșitul lui 2008) se răspândește autonom, utilizând în acest scop o vulnerabilitate din serviciul de sistem, care este răspunzător, printre altele, de partajarea de fișiere și directoare în rețea.

O a doua variantă, numită Downadup.B, a reușit să ia cu asalt internetul, dar mai ales rețelele interne ale corporațiilor, răspândindu-se cu repeziciune și ajungând la nivel de epidemie, din cauza unor modificări ale codului său, dar și a faptului că întreprinderile și instituțiile mari nu aplicaseră încă patch-ul care rezolva vulnerabilitatea. Astfel, virusul s-a putut răspândi nestingherit prin fișiere partajate sau „călătorind" pe stick-uri de memorie USB infectate între un calculator și altul.

Lipsa unei soluții de securitate care să alerteze utilizatorii asupra necesității unui patch și să poată bloca pro-activ infectarea a completat tabloul, astfel ca Downadup ar putea intra în „galeria" celor mai periculoși viruși ai noului secol, alături de Storm sau chiar de SQL Slammer.

BitDefender a creat o unealtă specializată pentru dezinfectarea acestui virus, dar aceasta nu poate proteja împotriva unei re-infectări sau a unor noi variante ale virusului. Produsele de securitate BitDefender au însă această capacitate. Specialiștii au creat chiar și o „semnătură generică", astfel încât acestea sunt capabile să detecteze și eventuale variante viitoare ale virusului, nu numai pe cele deja existente.

Din păcate, este evident că Downadup nu este și singura amenințare informatică cu care se vor confrunta internauții și firmele care își desfășoară activitatea cu ajutorul internetului în acest an, dar toate aceste probleme de securitate IT își pot găsi răspunsurile în soluțiile oferite de BitDefender prin gama de produse lansate pentru 2009.

Ideal pentru familiile „conectate la net", BitDefender Total Security 2009 oferă protecție proactivă complexă pentru calculatorul tău, fără a reduce viteza acestuia. Soluția include antivirus, antispyware, antispam și firewall oferind protecție eficientă împotriva atacurilor informatice și a altor amenințări de pe Internet. Foarte importantă este funcția de backup care te ajută să îți păstrezi documentele și datele confidențiale în completă siguranță.

Pentru toate companiile care doresc să asigure protecția datelor clienților și a informațiilor confidențiale proprii, precum și evitarea întreruperilor de activitate datorate infecțiilor în rețea, a fost dezvoltat BitDefender Corporate Security, o soluție de securitate și administrare robustă și ușor de folosit, care oferă protecție superioară împotriva virușilor, a programelor spion, a rootkit-urilor, a mesajelor de tip spam, a tentativelor de fraudare de tip phishing și a altor programe periculoase.

BitDefender Corporate Security sporește productivitatea companiei și reduce costurile legate de administrarea rețelei și de securitate a datelor prin funcționalități de management centralizat, protecție împotriva pericolelor informatice și, nu în ultimul rând, de control asupra calculatoarelor din rețeaua proprie.

La baza tuturor produselor BitDefender stă tehnologia B-HAVE, o metodă de detecție proprie în curs de brevetare, care constă în analizarea, în interiorul unui calculator virtual, a comportamentului aplicațiilor cu potențial periculos. În acest fel, se elimină alarmele false și crește simțitor rata de detecție a pericolelor noi și necunoscute, iar pentru a oferi o soluție mai bună la problema noilor valuri de spam, laboratoarele BitDefender au creat NeuNet, un filtru antispam puternic. NeuNet „învață" în laboratorul antispam caracteristicile mesajelor de acest fel și folosește, apoi, aceste tipare pentru identificarea noilor mesaje spam.