BITDEFENDER ASIGURĂ PROTECȚIE ÎN MEDIUL VIRTUAL

Pionier autohton în domeniul soluțiilor de securitate, BitDefender este una dintre cele mai cunoscute companii româneşti pe plan internațional. Din laboratoarele BitDefender au ieşit, în ultimii 8 ani, cei mai performanți luptători împotriva amenințărilor informatice, adevărați paznici virtuali înzestrați cu inteligență artificială.

Sorin Titus IORDAN

BitDefender elaborează periodic un raport al celor mai periculoase amenințări informatice şi al celor mai folosite metode de fraudare. Specialiştii BitDefender au remarcat că în primele şase luni ale lui 2008, utilizatorii internet au fost nevoiți să facă față zilnic la aproximativ 2.000 de noi viruşi sau mutații ale acestora, la 50.000 de atacuri de phishing pe lună şi la peste 1.000.000 de calculatoare compromise, ce răspândesc bots sau rootkits, troieni sau alte forme de malware.
Vlad Vâlceanu, Head of Antispam, BitDefender, face lumină într-un subiect din ce în ce mai fierbinte: phishingul.

Care a fost evoluția tentativelor de phishing anul trecut?

Înțeles ca o activitate ilegală, phishingul reprezintă încercarea de a obține informații personale şi confidențiale, precum numele de utilizatori, parole, numere de identificare personală sau numerele cărților de credit, prin crearea unor mesaje e-mail false, care pretind că aparțin unei entități legitime. În atacurile de phishing nu sunt vizate băncile, ci clienții acestora, oameni care dețin conturi în băncile respective şi folosesc des serviciile de internet banking.
În 2008, ținând cont de numărul de atacuri (nu de cantitatea e-mailurilor), peisajul autohton a dezvăluit că industria de phishing capătă amploare. Sporirea numărului de conexiuni la internet şi folosirea tot mai des a serviciilor de e-banking a adus în prim-plan noi şi îmbunătățite tehnici de phishing, care i-au vizat pe clienții Raiffeisen Bank (50%), BCR (17%), BRD (13%), Piraeus Bank (10%) şi Banca Transilvania (10%). Cu toate acestea, phishingul nu se limitează doar la clienții unor bănci, ci îi vizează şi pe clienții care preferă serviciile online, precum eBay®, PayPal™, Amazon.com®, AOL®, AT&T® sau Orange™. Activitățile de phishing se bazează pe un tipar simplu. De obicei, autorii de phishing folosesc valuri uriaşe de e-mailuri pentru a păcăli presupusele victime să divulge informațiile private. Cele mai multe argumente invocate în mesajele false sunt negative, precum faptul că un cont a fost blocat sau a expirat. Oricare ar fi motivele invocate, autorii de phishing vor goli cu siguranță conturile bancare, dacă dispun de aceste informații.

Cum se pot proteja utilizatorii de asemenea atacuri?

Autorii mizează pe mesaje cu hyperlink către serverul în care se înregistrează numele de utilizator, parola de acces şi seria cardului. Altă metodă preferată este ataşarea unei pagini HTML care înregistrează informațiile private şi le trimite printr-un script PHP către o bază de date aflată la distanță. Pentru că spamul prin e-mail joacă un rol esențial în aceste campanii de phishing, utilizatorii sunt sfătuiți să urmeze câteva reguli elementare:
• să nu răspundă solicitărilor trimise prin astfel de mesaje. Mesajele emise de instituțiile financiare sunt personalizate şi nu fac obiectul unei expedieri în masă, acestea fiind cel mai adesea trimise prin serviciile de poştă sau de curierat, nu prin e-mail.
• să nu furnizeze date confidențiale prin intermediul unor pagini HTML anexate, chiar dacă, aparent, par a proveni de la bancă.
• în momentul primirii unui astfel de e-mail, să contacteze de urgență banca şi să o informeze despre tentativa de phishing, solicitând detalii despre măsurile de protecție adecvate.
• pentru prevenirea pierderii datelor confidențiale şi, în ultimă instanță, a sumelor din conturi, să instaleze o suită de securitate care să includă module Antispam, Antiphishing şi Antimalware, precum cea oferită de BitDefender®, care detectează şi blochează cu succes această amenințare.

Care sunt atuurile BitDefender în competiția cu ceilalți dezvoltatori de soluții de securitate?

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 şi creşte simțitor rata de detecție a pericolelor noi şi 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 şi foloseşte, apoi, aceste tipare pentru identificarea noilor mesaje spam. Teste independente internaționale efectuate în ianuarie 2008 de laboratoarele de Testare Anti-Malware au indicat faptul că tehnologia BitDefender euristică B-HAVE detectează 63% din e-amenințări, fără a fi nevoie de o semnătură suplimentară.