ATENȚIE LA PHARMING!

de Alexandru Catalin COȘOI
Senior Researcher
Laboratorul AntiSpam BitDefender

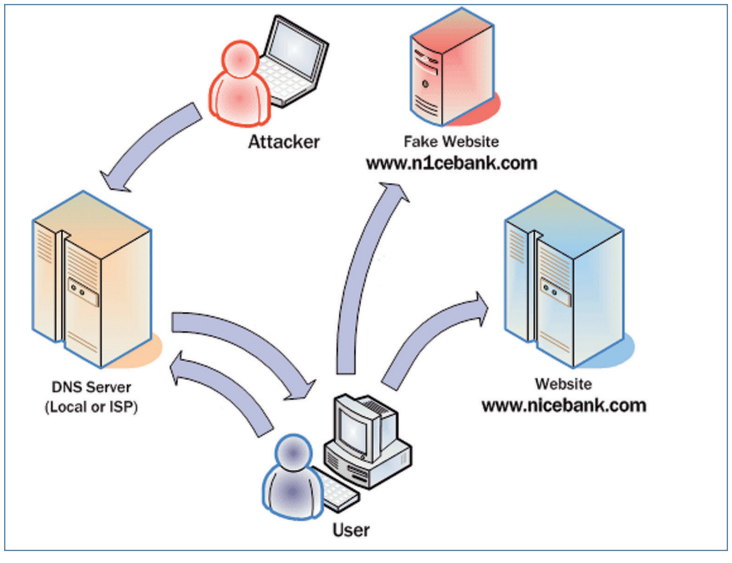
Suntem convinşi că un număr tot mai mare de utilizatori ai Internetului ştiu deja ce este phishing-ul şi care sunt modalitatile în care pot evita să-i pice în plasa. O schemă tipică de înşelăciune de gen phishing operează ca "Bonnie and Clyde" modern, compusă dintr-un e-mail ilegal, susţinut de un site compromis. E-mailul fraudulos, venit din partea unei binecunoscute companii sau instituţii financiare, are ca scop păcălirea destinatarilor în accesarea diverselor link-uri pe care le conţin către site-uri compromise şi obtinerea pe această cale a informaţiilor private ale utilizatorilor.

Verişorul primar şi mai sofisticat al phishing-ului este o tehnica denumită "pharming". Ca şi phishing-ul, pharming-ul încearcă să păcălească utilizatorul să viziteze un anumit site şi să sustragă informaţii confidenţiale. Cu toate acestea, în loc de a păcăli destinatarii să acceseze un link dintr-un e-mail, pharmingul poate redirecţiona în secret victimele către un site compromis direct din browserul web folosit de aceştia. Astfel, pharming-ul elimină definitiv existenţa unui e-mail ca "momeala" şi este în consecinţă mult mai periculos decât tehnicile uzuale de phishing, putând atinge o gamă mai largă de victime. Chiar şi un utilizator de Internet cunoscător în ale phishing-ului poate cădea cu uşurinţă victima unei tentative de pharming, fără ca măcar să-şi dea seama, iar posibilitatea ca userul să ignore atenţionarea unei soluţii de securitate este cu atât mai mare cu cât pagina către care va fi redirecţionat va imita toate caracteristicile paginii oficiale ale băncii.

Pentru succesul unei scheme de pharming, autorii acesteia pot compromite direct sistemul viitoarei victime prin instalarea în mod secret a unei aplicaţii software infectate (lucru care o poate face chiar userul, instalându-şi un program gratuit disponibil online pe un site maliţios) sau prin modificarea fişierelor de host ale browser-ului folosit de utilizator. În mod alternativ, autorii pot folosi chiar "DNS cache poisoning" pentru a compromite eficient şi serverul DNS.

Un server DNS (Domain Name Service) este răspunzător pentru traducerea adreselor internet dintr-un format plăcut ochiului într-o adresă tip masina (IP). Astfel, când utilizatorul va introduce în browser adresa "www.banca.ro", browserul va trimite această adresă către serverul său DNS, iar acesta îi va răspunde cu adresa IP de unde se poate încărca pagina corespunzătoare adresei respective. Pentru a nu se efectua de fiecare dată căutarea, fiecare server DNS are un cache unde sunt păstrate cele mai accesate adrese pentru a putea răspunde mai repede. Un hacker se poate folosi de diverse vulnerabilităţi pentru a compromite acest cache şi, astfel, serverul va întoarce alt IP, acela al phisherului, unde se va găsi o clonă identică a site-ului băncii. Inclusiv linkul în bara de adrese este acelasi şi, de aceea, este foarte probabil ca utilizatorii să ignore aceste alerte.

În traducere libera, chiar daca introduci manual adresa web a băncii tale sau a instituţiei financiare direct în browser, sau o accesezi prin cele mai recente bookmark-uri folosite anterior, este foarte posibil ca un atac de pharming sa redirectioneze browser-ul, fără să-ţi dai seama, către un site compromis. Dacă acesta este realizat după „chipul si asemănarea" celui original, utilizatorul îsi poate insera liniştit datele de acces la cont, parola şi alte informaţii confidenţiale fără să-şi dea seama ce se întâmplă.



Momentan, la nivel mondial, pharming-ul nu este la fel de raspândit ca phishing-ul, deoarece, dacă un atac de phishing necesită un nivel de cunoştinţe de rang 2 (pe o scara de la 1 la 10), pentru un atac de pharming este necesar un nivel de aproape 7. Cu toate acestea, multi experţi în securitatea informatică prevestesc faptul că atacurile de pharming vor creşte în amploare pe măsură ce tot mai mulţi autori de e-ameninţări vor prefera mai degrabă aceasta tehnica, decât phishing-ul.

Pentru a vă asigura că nu sunteţi victima unui atac de pharming, fiţi siguri că aveţi o soluţie de securitate care să conţină un antivirus (pentru a evita instalarea de programe maliţioase în calculatorul dumneavoastră), antispyware, un firewall şi, bineînteles, o soluţie antiphishing care se integrează cu browserul folosit, fiind de preferat o soluţie capabilă să determine şi atacuri de tip pharming.