

Hackeri

Ce sunt hackerii ?

Hackerii sunt pasionați ai informaticii, care, de obicei au ca scop „spargerea” anumitor coduri, baze de date, pagini web etc. Ei sunt considerați infractori, în majoritatea statelor lumii. Hackerii adevărați nu „distrug”, de obicei, pagini inofensive, cum ar fi paginile personale. Țintele obișnuite ale atacurilor hackerilor sunt sistemele importante, care au protecții avansate și conțin informații strict secrete, cum ar fi bazele de date ale Pentagonului sau cele de la NASA. Odată obținute, aceste fișiere (informații) sunt publicate pe tot Internet-ul, pentru a fi vizionate sau folosite de cât mai multe persoane.

Orice hacker advărat trebuie să respecte un „Cod de legi al hackerilor”, care este bine stabilit, cunoscut și respectat.

Hackeri amatori

Există „hackeri” care atacă ținte aleatoare, oriunde și oricând au ocazia. De exemplu, atacurile tot mai frecvente asupra Yahoo și Hotmail au blocat motoarele de căutare și conturile de mail respective pentru câteva zile, aducând prejudicii de milioane de dolari.

Aceste atacuri (care reprezintă o încălcare destul de gravă a „Codul de legi al hackerilor”) au de obicei în spate persoane care „au fost curioși numai să vadă ce se întâmplă” sau „au dorit să se distreze”. Acești atacatori virtuali nu sunt hackeri adevărați, pentru că nu-și scriu singuri nuke - urile (programele pentru bombardare - nucleare) pe care le folosesc, procurându-și-le de pe Internet sau din alte surse.

Acești hackeri amatori sunt singurii care ajung în fața justiției. Motivul este simplu. Acei hackeri adevărați care își pot scrie singuri nuke - urile, sunt, de obicei destul de inteligenți pentru a face anumite sisteme care să inducă în eroare pe toți aceia care ar încerca să determine sursa atacului.

Crackeri

Crackerii reprezintă un stil anumit de hacker, care sunt specializați în „spargerea” programelor shareware, sau care necesită un anumit cod serial. Singurii care sunt prejudiciați de această categorie de hackeri sunt cei care scriu și proiectează programele „sparte”.

Sistemele de protecție ale aplicațiilor respective pot fi „înfrânte” prin două metode:

Introducerea codului, care poate fi găsit fie pe Internet, fie cu ajutorul unui program asemănător cu OSCAR 2000, care este o bibliotecă de coduri.

A doua metodă este folosită pentru sistemele de protecție mai avansate, care necesită chei hardware (care se instalează pe porturile paralele ale computerului și trimit un semnal codat de câte ori le este cerut de către programul software), sunt patch-urile. Ele sunt programele care sunt făcute special pentru anumite aplicații software, care odată lansate modifică codul executabil, inhibând instrucțiunile care cer cheia hardware.

Patch-urile și bibliotecile de coduri seriale se găsesc cel mai des pe Internet. Ele sunt făcute de anumite persoane (care sunt câteodată foști angajați ai firmelor care au scris software-ul respectiv) care vor doar să aducă pagube firmei proiectante.

Deși pare ciudat, cracking - ul este considerată „piraterie computerizată”, reprezentând o infracțiune serioasă. Totuși, foarte rar sunt depistați cei care plasează patch-uri și coduri seriale pe Internet.

Setul de unelte al unui hacker

Precum am mai precizat, hackerii adevărați își scriu singuri software-ul ce le e necesar. Multe dintre aceste programe, după ce sunt testate, sunt publicate pe Internet. Bineînțeles, programele folosite pentru „spargerea” serverelor de la Pentagon sau pentru decodarea fișierelor codate pe 64 biți nu se vor găsi așa de ușor pe Net, ele fiind ținute secrete de realizatorii lor.

Prezentăm în continuare câteva dintre programele pentru hackerii amatori:

BoGUI BackOrifice. Un produs al The Dead Cow Cult, Bogui reprezintă un program de control al computerelor din rețeaua dumneavoastră locală. Comenzi ca System Lockup (sau Restart) nu-l vor prea bine dispune pe utilizatorul computerului țintă. Singura problemă a acestui program este că toate comenzile sunt pachete transmise unui virus troian, astfel încât, dacă computer-ul destinație nu este infectat, bombardamentul cu Back Orifice nu va avea nici un efect.

Net Nuke. Acest program are o mulțime de versiuni, deși toate au același efect și mod de operare: trimit un pachet nedefragmentabil prin rețea, astfel încât când computer-ul țintă va încerca să-l defragmenteze, nu va reuși decât să blocheze portul de rețea.

Mail Nukers. Sunt programe care bombardează o casuță de poștă electronică cu un număr mare de mesaje (care de obicei depășește 10000). Acest bombardament duce la blocarea sau chiar pierderea unei casuțe de e-mail. Majoritatea acestor programe au opțiuni care permit trimiterea de mail-uri anonime.

Aceste programe pot fi procurate de către oricine foarte ușor de pe Internet. Din păcate, unele dintre ele sunt folosite și ca un mediu de răspândire a virușilor, care pot avea efecte secundare foarte grave. Oricum, nu este recomandată abuzarea de aceste programe sau folosirea lor în scopuri (prea) distrugătoare.

Mass E - Mail-eri

Mass E - Mail-eri sau spameri sunt acei hackeri care transmit cantități enorme de e-mail (sau alt fel de informații), conținând oferte nesolicitate, sau informații aleatoare, transmise în scopul de a bloca anumite servere. Majoritatea site-urilor importante cum ar fi Yahoo, Amazon.com sau Hotmail au anumite sisteme de filtrare care ar trebui să protejeze serverele respective de atacurile cu cantități enorme de informații. Aceste capcane sunt însă ușor de evitat chiar și de începătorii în domeniul hackingului.

În ultimul timp serverele precizate mai sus precum și multe altele au fost supuse la puternice „atacuri cu informații”, la care nu puteau face față. S-au trimis mesaje la o capacitate de aproape un MB/secundă, deși serverele respective suportau un trafic obișnuit de până la 1 - 1,5 GB săptămânal.

Spamerii, prin atacurile lor prejudiciază cu sute de milioane de dolari serverelor țintă. Tot odată sunt afectați și utilizatorii serverelor respective, traficul fiind complet blocat, trimiterea sau primirea mesajele sau utilizarea altor servicii asemănătoare fiind imposibilă.

Vă întrebați cum se pot trimite cantități atât de mari de informații, la o viteză uimitoare, fără ca hackerii respectivi să fie localizați fizic. Este relativ simplu pentru ei: transmit mesajele de pe aproximativ 50 de adrese de mail, după care deviază informația transmisă prin mai multe puncte din lume (diferite servere). Astfel, este foarte de greu să fie detectați, echipele de specialiști de la FBI lucrând săptămâni (chiar luni) întregi pentru a prinde infractorul virtual, de multe ori neajungând la rezultate concrete.

Singura problemă (a hackerilor) care apare în cazul acestor devieri succesive ale informației este aceea că unul din serverele prin care „trece” informația în drumul ei către „ținta” finală se poate bloca. Informația nu va ajunge în întregime la destinație, puterea atacului scăzând substanțial. Astfel de cazuri se pot considera atacurile din ultimul timp, serverele afectate nefiind cele vizate de hackeri.

Protecții

Dacă într-o zi chiar dumneavoastră veți fi una dintre nefericitele victime ale atacului unui hacker răutăcios? Cum vă puteți apăra rețeaua, baza de date sau pagina de pe web ?

Acestea probleme sunt importante pentru foarte mulți utilizatori de computere, care utilizează în mod regulat Internet-ul. Există protecții împotriva atacurilor hackerilor. Singura problemă este aceea că regulile și protecțiile sunt făcute pentru a fi încălcate.

Deci, oricât de complexe și de sigure ar părea sistemele dumneavoastră de securitate, ele pot fi ocolite și „sparte”.

Există totuși anumite metode care, deocamdată, ar putea îngreuna puțin viața hackerilor, mai ales a spammeriilor (acesta fiind cel mai folosit în ultimul timp). Aceste ar trebui în primul rând aplicate de providerii de Internet (ISP):

Vă trebui eliminate toate fișierele necunoscute de pe servere (care ar ușura atacurile hackerilor), astfel încât se va ține o strictă evidență a lor.

Eliminarea pachetelor care au alt header decât propria adresă de IP (pachete măsluite). Ele pot fi folosite de unii utilizatori sub pretextul necesității anonimatului. Există însă alte modalități de ați păstra anonimatul, folosind sisteme de criptare și a unor servere specializate.

Interzicerea comportamentelor specifice scanării porturilor. Astfel se pot dezactiva programele care scanează zeci de mii de porturi din întreaga lume, pentru a face o listă cu cele vulnerabile.

Scanarea atentă a serverelor de „sniffere”, programele care rețin informațiile importante care intră și ies dintr-un server (username-uri, parole, numere de cărți de credit etc). Pe lângă metodele de protecție prezentate mai sus există și multe multe altele, mai mult sau mai puțin vulnerabile.

În orice caz, până la aducerea securității la un nivel acceptabil mai este mult de lucru...

Concluzii

Ce sunt hackerii cu adevărat ? Ce vor ei de fapt ? Acestea sunt întrebări la care numai un hacker adevărat poate răspunde (ceea ce nu se întâmplă prea des).

Vom încerca totuși să explicăm câteva din scopurile lor:

Adevăr. Mulți dintre hackeri „sparg” cele mai ciudate și complexe coduri de la Pentagon și NASA în speranța ca vor reuși să demonstreze existența „omuleților verzi” sau a altor „teorii ale conspirației”

Superioritate. Demonstrarea superiorității lor față de „marii” programatori, sistemele informatice și serverele care le aparțin este scopul multor hackeri.

Distrație. Unii hackerii fac „distrugeri” masive doar pentru a se distra pe seama celor care își văd munca distrusă în câteva secunde.

Protest. „Distrug” anumite site-uri de web sau baze de date fiindcă nu sunt de acord cu informația transmisă de ele.

Bani. Uneori se „sparg” bazele de date de la bănci, pentru a transfera câteva milioane de dolari în contul propriu. Aceste operațiuni sunt foarte riscante, necesită experiență în domeniu, nefiind încercate de prea mulți hackeri.

Anumiți hackeri, care au demonstrat de ce sunt în stare, fără a aduce pagube semnificative, devin consultanți în probleme de securitate computerizată. Ei poartă numele de „hackeri în alb”. În câteva luni se va descoperi o nouă metodă de hacking care să depășească cu mult cunoștințele hackerului respectiv. Concluzia că hackerii sunt „o specie ce nu poate evolua în captivitate”.

Într-adevăr, „viața de hacker” este foarte incitantă, tentantă, nostimă și interesantă, dar în același timp foarte riscantă și periculoasă. Majoritatea statelor lumii consideră hackingul o infracțiune foarte gravă, pentru care pedeapsa meritată este considerată de obicei interzicerea folosirii computerului, în unele cazuri, chiar ... PENTRU TOT RESTUL VIEȚII!!!