Hackerii

Ce sunt hackerii ?

Hackerii sunt pasionaţi ai informaticii, care, de obicei au ca scop „spargerea" anumitor coduri, baze de date, pagini web etc. Ei sunt consideraţi infractori, în majoritatea statelor lumii. Hackerii adevăraţi nu „distrug", de obicei, pagini inofensive, cum ar fi paginile personale. Ţintele obişnuite ale atacurilor hackerilor sunt sistemele importante, care au protecţii avansate şi conţin informaţii strict secrete, cum ar fi bazele de date ale Pentagonului sau cele de la NASA. Odată obţinute, aceste fişiere (informaţii) 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 şi respectat.

Hackeri amatori

Există „hackeri" care atacă ţinte aleatoare, oriunde şi oricând au ocazia. De exemplu, atacurile tot mai frecvente asupra Yahoo şi Hotmail au blocat motoarele de căutare şi 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 curioşi numai să vadă ce se întâmplă" sau „au dorit să se distreze". Aceşti atacatori virtuali nu sunt hackeri adevăraţi, pentru că nu-şi scriu singuri nuke – urile (programele pentru bombardare - nucleare) pe care le folosesc, procurându-şi-le de pe Internet sau din alte surse.
Aceşti hackeri amatori sunt singurii care ajung în faţa justiţiei. Motivul este simplu. Acei hackeri adevăraţi care îşi pot scrie singuri nuke – urile, sunt, de obicei destul de inteligenţi pentru a face anumite sisteme care să inducă în eroare pe toţi aceea care ar încerca să determine sursa atacului.

Crackeri

Crackerii reprezintă un stil anumit de hacker, care sunt specializaţi în „spargerea" programelor shareware, sau care necesită un anumit cod serial. Singurii care sunt prejudiciaţi de această categorie de hackeri sunt cei care scriu şi proiectează programele „sparte".
Sistemele de protecţie ale aplicaţiilor 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 protecţie mai avansate, care necesită chei hardware (care se instalează pe porturile paralele ale computerului şi trimit un semnal codat de câte ori le este cerut de către programul software), sunt patch-urile. Ele sunt progrămele care sunt făcut special pentru anumite aplicaţii software, care odată lansate modifică codul executabil, inhibând instrucţiunile care cer cheia hardware.

Patch-urile şi bibliotecile de coduri seriale se găsesc cel mai des pe Internet. Ele sunt făcute de anumite persoane (care sunt câteodată foşti angajaţi ai firmelor care au scris software-ul respectiv) care vor doar să aducă pagube firmei proiectante.
Deşi pare ciudat, cracking – ul este considerată „piraterie computerizată", reprezentând o infracţiune serioasă. Totuşi, foarte rar sunt depistaţi cei care plasează patch-uri şi coduri seriale pe Internet.

Setul de unelte al unui hacker

Precum am mai precizat, hackerii adevăraţi îşi scriu singuri software-ul ce le e necesar. Multe dintre aceste programe, după ce sunt testate, sunt publicate pe Internet. Bineînţeles, programele folosite pentru „spargerea" serverelor de la Pentagon sau pentru decodarea fişierelor codate pe 64 biţi nu se vor găsi aşa de uşor pe Net, ele fiind ţinute 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 reţeaua dumneavoastră locală. Comenzi ca System Lockup (sau Restart) nu-l vor prea bine dispune pe utilizatorul computerului ţintă. Singura problemă a acestui program este că toate comenzile sunt pachete transmise unui virus troian, astfel încât, dacă computer-ul destinaţie nu este infectat, bombardamentul cu Back Orifice nu va avea nici un efect.
- Net Nuke. Acest program are o mulţime de versiuni, deşi toate au acelaşi efect şi mod de operare: trimit un pachet nedefragmentabil prin reţea, astfel încât când computer-ul ţintă va încerca să-l defragmenteze, nu va reuşi decât să blocheze portul de reţea.
- Mail Nukers. Sunt programe care bombardează o căsuţă de poştă electronică cu un număr mare de mesaje (care de obicei depăşeşte 10000). Acest bombardament duce la blocarea sau chiar pierderea unei căsuţe de e-mail. Majoritatea acestor programe au opţiuni care permit trimiterea de mail-uri anonime.

Aceste programe pot fi procurate de către oricine foarte uşor de pe Internet. Din păcate, unele dintre ele sunt folosite şi ca un mediu de răspândire a viruşilor, 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 cantităţi enorme de e-mail (sau alt fel de informaţii), conţinând oferte nesolicitate, sau informaţii 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 cantităţi enorme de informaţii. Aceste capcane sunt însă uşor de evitat chiar şi de începătorii în domeniul hackingului.

În ultimul timp serverele precizate mai sus precum şi multe altele au fost supuse la puternice „atacuri cu informaţii", la care nu puteau face faţă. S-au trimis mesaje la o capacitate de aproape un MB/secundă, deşi serverele respective suportau un trafic obişnuit de până la 1 – 1,5 GB săptămânal.

Spamerii, prin atacurile lor prejudiciază cu sute de milione de dolari serverelor ţintă. Tot odată sunt afectaţi şi utilizatorii serverelor respective, traficul fiind complet blocat, trimiterea sau primirea mesajele sau utilizarea altor servicii asemănătoare fiind imposibilă.

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

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

Protecţii

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

Acestea probleme sunt importante pentru foarte mulţi utilizatori de computere, care utilizează în mod regulat Internet-ul. Există protecţii împotriva atacurile hackerilor. Singura problemă este aceea că regulile şi protecţiile sunt făcute pentru a fi încălcate.

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

Există totuşi anumite metode care, deocamdată, ar putea îngreuna puţin viaţa hackerilor, mai ales a spammeri-lor (acesta fiind cel mai folosit în ultimul timp). Aceste ar trebui în primul rând aplicate de providerii de Internet (ISP):

- Va trebui eliminate toate fişierele necunoscute de pe servere (care ar uşura atacurile hackerilor), astfel încât se va ţine o strictă evidenţă a lor.
- Eliminarea pachetelor care au alt header decât propria adresă de IP (pachete măsluite). Ele pot fi folosite de unii utilizatori sub pretextul necesitării anonimatului. Există însă alte modalităţii de aţi păstra anonimatul, folosind sisteme de criptare şi 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 reţin informaţiile importante care intră şi ies dintr-un server (username-uri, parole, numere de cărţi de credit etc).

Pe lângă metodele de protecţie prezentate mai sus există şi multe multe altele, mai mult sau mai puţin vulnerabile.

În orice caz, până la aducerea securităţii 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 totuşi să explicăm câteva din scopurile lor:

- Adevăr. Mulţi dintre hackeri „sparg” cele mai ciudate şi complexe coduri de la Pentagon şi NASA în speranţa ca vor reuşi să demonstreze existenţa „omuleţilor verzi” sau a altor „teorii ale conspiraţiei”
- Superioritate.Demonstrarea superiorităţii lor faţă de „marii” programatori, sistemele informatice şi serverele care le aparţin este scopul multor hackeri.
- Distracţie. Unii hackerii fac „distrugeri” masive doar pentru a se distra pe seama celor care îşi văd munca distrusă în câteva secunde.
- Protest. „Distrug” anumite site-uri de web sau baze de date fiindcă nu sunt de acord cu informaţia transmisă de ele.

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

Anumiţi hackeri, care au demonstrat de ce sunt în stare, fără a aduce pagube semnificative, devin consultanţi 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 depăşească cu mult cunoştiinţele hackerului respectiv. Concluzia că hackerii sunt „o specie ce nu poate evolua în captivitate”.

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