Poate cel mai temut hacker din SUA, Rob Joyce, șeful echipei de hackeri a Agenției Naționale americane pentru Securitate (National Security Agency - NSA), a explicat într-un discurs rostit în cadrul primei ediții a conferinței de securitate cibernetică Usenix Enigma, desfășurată în perioada 25-27 ianuarie la San Francisco, ce măsuri trebuie să ia administratorii de sisteme informatice dar și utilizatorii obișnuiți pentru a se feri de hackeri, conform unui material publicat de site-ul wired.com.

Rob Joyce este șeful grupului operațional Tailored Access Operations (TAO), echipa de hackeri de care dispune NSA și care trebuie să spargă sistemele informatice ale adversarilor Washingtonului și, ocazional, notează wired.com. și pe cele ale aliaților SUA. Joyce lucrează în cadrul NSA de peste 25 de ani și a devenit șeful TAO din aprilie 2013, cu doar câteva săptămâni înainte de celebrul scandal declanșat de Edward Snowden și de scurgerea de informații clasificate spre publicații precum The Guardian și Washington Post.

Joyce a recunoscut că este puțin bizar ca un hacker să fie poftit să susțină o conferință despre metodele pe care le folosește pentru a sparge sistemele informatice. Grupul operațional TAO era o divizie secretă a NSA. Existența sa, doar bănuită, a fost confirmată de documentele publicate de Snowden. Joyce s-a ferit însă să facă referiri la operațiunile desfășurate de TAO și, în schimb, a expus un mic compendiu cu privire la cele mai bune măsuri ce pot fi luate pentru securizarea informațiilor digitale.

Conform șefului hackerilor din cadrul NSA, ținta predilectă a piraților informatici nu sunt VIP-urile unei organizații (conducerea respectivei organizații), ci tocmai administratorii rețelei informatice și alte persoane din cadrul organizației care au privilegii de acces la rețea. Cu alte cuvinte, hackerii NSA îi vânează direct pe administratorii de sistem ai unei organizații pentru a-și asigura accesul complet și cât mai discret asupra conținutului online.

De asemenea, hackerii NSA caută parole hardcoded în software sau transmise în clar — în special în cadrul protocoalelor de securitate mai vechi — care odată sparte deschid accesul pe orizontală printr-o rețea informatică. Nicio vulnerabilitate informatică nu este prea puțin semnificativă pentru a fi exploatată de hackerii NSA.

"Să nu vă închipuiți că un anumit crack este prea mic pentru a fi remarcat sau prea nesemnificativ pentru a fi exploatat", a avertizat el. Dacă operezi un test de penetrare a propriei rețele și rezultatele indică, spre exemplu, că 97% dintre barierele de securitate rezistă, dar, aparent, cele mai neînsemnate 3% pot fi penetrate, atunci acestea pot constitui vulnerabilitățile care să compromită întregul sistem de securitate. Hackerii NSA și cei care lucrează pentru alte state caută în permanență să infiltreze astfel de puncte de vulnerabilitate aparent insignifiante. Chiar și crack-urile temporare — vulnerabilități ale unui sistem care pot persista pentru doar câteva ore sau zile — pot fi exploatate de hackerii care, odată pătrunși în sistem, rămân acolo chiar și după îndepărtarea acestor vulnerabilități.

Spre exemplu, dacă o anumită aplicație din rețea nu funcționează cum ar trebui, iar compania care a construit sistemul informatic îți solicită să-l lași accesibil la sfârșit de săptămână pentru ca experții săi în IT să poată remedia problema, o astfel de situație reprezintă o invitație pentru

hackerii care oricum testează permanent permeabilitatea sistemelor informatice pe care încearcă să le infiltreze.

Există și alte vulnerabilități exploatate cu predilecție de către hackeri. Spre exemplu, dispozitivele sau gadgeturile personale introduse de angajați într-o agenție, companie sau departament guvernamental și pe care le conectează la rețeaua de la locul de muncă. Dacă pe aceste dispozitive mobile sunt instalate și jocuri online, cu atât mai bine.

Alte vulnerabilități la care ne-am aștepta mai puțin sunt reprezentate de sistemele de încălzire și de aclimatizare ale clădirii, sau de alte sisteme care țin de infrastructură ce pot deschide portițe pentru hackeri.

Rob Joyce nu s-a referit însă și la alte modalități prin care hackerii NSA pot penetra sistemele informatice, așa cum este tehnica de injectare de cod Quantum, care i-a permis agenției americane să spargă sistemele de securitate ale companiei belgiene de telecomunicații Belgacom, mai notează wired.com.

În general, a subliniat Joyce, piraților informatici nu au probleme foarte mari în accesarea unei anumite rețele de interes pentru ei pentru că își dedică suficient timp acestui lucru și ajung să cunoască respectiva rețea chiar mai bine decât persoanele autorizate să opereze respectiva rețea.

"Noi alocăm suficient timp pentru a ajunge să cunoaștem o rețea mai bine (chiar) decât cei care au construit-o și decât cei angajați să-i asigure securitatea. Ei știu ce au vrut să facă într-o rețea, pe când noi cunoaștem exact ce au reușit să facă. Există o diferență subtilă. Ați fi surprinși să aflați ce diferențe pot exista între lucrurile care chiar funcționează într-o rețea și lucrurile despre care voi credeți că funcționează într-o rețea", a susținut el.

În continuare, Joyce a oferit o serie de sfaturi pentru cei care doresc să le îngreuneze viața hackerilor, fie ei guvernamentali, angajați de companii sau corporații sau independenți. În primul rând, trebuie limitate privilegiile de acces la rețea pentru sistemele importante doar la persoanele care chiar trebuie să le acceseze. De asemenea, rețelele și datele importante trebuie segmentate pentru a fi mai greu accesate în totalitatea lor. Sistemele trebuie să primească patch-uri de securitate în mod regulat și trebuie să se renunțe la parolele hardcoded (scrise în codul aplicației care solicită autentificarea) și la protocoalele de bază care transmit parola în clar în rețea.

Un veritabil coșmar pentru hackeri este un dispozitiv de tipul 'out-of-band network tap' — dispozitiv care monitorizează activitatea pe rețea și produce documente (logs) care înregistrează orice activitate suspectă sau orice anomalie din rețea — desigur însă că un astfel de sistem de securitate are nevoie de niște administratori de sistem care să și citească cu atenție log-urile generate, pentru a identifica orice mișcare suspectă.

Contrar părerii împărtășite de mulți, NSA sau alt atacator de tip APT (Advanced Persistent Threat — un set de procese de hacking ascunse și continue) nu se bazează prea mult pe așa-numitele "zero-day exploits" — breșe de securitate ale unui software abia lansat, de care

producătorul respectivului software nu este încă conștient și care pot fi exploatate deseori de hackeri înainte să fie acoperite de patch-uri ulterioare.

"Orice rețea mare poate fi penetrată cu răbdare și concentrare, chiar și fără a profita de breșe de tipul 'zero-day exploits'. Există foarte multe abordări posibile care sunt mai ușoare, mai puțin riscante și de multe ori mai productive decât apelul la breșele de tipul 'zero-day exploits'", a mai susținut el, adăugând că din această categorie fac parte și vulnerabilitățile cunoscute pentru care există patch-uri de securitate, dar care nu au fost încă instalate de către administratorii rețelei. AGERPRES