SECURITATEA ÎN TELECOMUNICAȚII

PREP. UNIV.ȚÎRLEA CAMELIA ADRIANA
Universitatea din Oradea, Facultatea de Ştiinţe Economice, str. Armatei Române, nr. 5, Telefon:0745-397486
E-mail: ctirlea@uoradea.ro

The development of the mobile phones in the last period, made from these phones real mini PCs, phenomena which could have a negative consequence. The endowment of these mobile phones with different operation systems, like Symbian, determined the exposure of these phones to the attack of viruses, especially created for these operation systems.

După probleme ca spyware, viruşi, troieni, si altele, producătorii de soft anti-virus se confruntă cu o nouă problemă, viruşii pe telefonia mobilă. Telefonia mobilă evoluează rapid, iar sistemele de operare pentru telefonul mobil nu mai reprezintă deja o noutate. În acelaşi timp hackerii devin din ce în ce mai interesaţi de modurile de a putea accesa informaţii aflate pe telefonul mobil.

Rezultatul este apariţia unor noi viruşi care pătrund în telefonia mobilă. După cum spune F-Secure, deocamdată există şase tipuri de baza de viruşi pentru telefoanele mobile, dar care se răspândesc în mai mult de 30 de variante. Toate acestea se întâmplă datorită faptului ca viruşii, mai precis codul sursă al acestora, a fost făcut public pe Internet.

Un alt motiv pentru cei care programează viruşi de a se implica în telefonia mobilă este efortul continuu dus pentru îmbunătăţirea securităţii calculatorului. Acest lucru a făcut mai dificilă scrierea unui virus pentru calculator decât a unuia pentru telefonul mobil.30 este un numar relativ mic comparativ cu cei aproximativ 120,000 de viruşi pentru PC-uri, însă acesta nu reprezintă un motiv pentru a nu preveni înmulţirea lor. Cateva din firmele de telefonie mobilă au semnat deja contracte cu mari companii ce produc anti-viruşi,

Calculatoarele cunosc bine aceste forme de agresiune, fie ele viermi, viruşi, cai troieni. După PC-uri, să fi devenit şi mobilele ţinta atacurilor hackerilor? În această lucrare voi încerca să evidenţiez diferenţa dintre pericolele reale şi alarmele false şi să prezint câteva modalităţi cu ajutorul cărora putem face faţă unor astfel de situaţii.

Mai de curând, după deficienţele de securitate ale standardului bluetooth şi atacurile pe SMS, primul vierme dezvoltat pentru mobile agită valurile din presă. Pe numele său Cabir, acesta apare pe paginile principale ale cotidianelor, invadează paginile de ştiri, diseminând frica şi prin intermediul televizorului. Şi totuşi, pe viu nu l-a „prins" încă nimeni, deoarece încă nu este în libertate. Cabir este mai mult un fel „Proof of Concept", realizat în laborator doar ca dovadă a faptului că viermii pentru telefoanele mobile sunt posibili şi vor exista. Pe acest fond, abia s-a auzit de existenţa lui Cabir, că specialiştii anti-virus oferă soluţii şi software aferent, pentru ca şansele pe viitor ale lui Cabir să fie egale cu zero.

Oricum, chiar în condiţiile în care Cabir ar scăpa, efectul lui n-ar fi nici pe departe atât de periculos pe cât de mari sunt temerile alimentate de presă. Spre deosebire de colegii săi din domeniul PC, viermele ce poate infecta aparatele din seria 60, bazate pe sistemul de operare Symbian, nu generează cu adevărat pagube mari: manifestările sale rezumându-se la transferul prin bluetooth pe alte aparate, golind rapid rezervele de energie ale acumulatorului. Îndepărtarea lui este mai simplă decât cea a unui vierme de pe calculator. Şi mai uşoară este profilaxia, pentru a împiedica infectarea soft-ului cu acest parazit. Motivul pentru care se face atâta vâlvă în jurul subiectului se datorează faptului că un asemenea fenomen era deja aşteptat de experţii în securitate, printre care şi Kevin Hogan. Conducătorul laboratorului dezvoltator de viruşi al firmei Symantec din Dublin a prezis de mult posibilitatea creării unor asemenea viruşi pentru telefoanele mobile. Experimentul Cabir va fi probabil semnalul de start al creşterii cererii pentru software de securitate al mobilelor. Nokia nu preia

responsabilitatea oferirii de aplicaţii de gen, ci indică programe antivirus pe care utilizatorii trebuie să şi le achiziţioneze singuri. În plus, protecţie reală împotriva viruşilor există doar în cazul actualizărilor la zi a programului. Se rezolvă astfel spinoasa problemă a aplicaţiei perfecte împotriva agresiunilor: cine doreşte securitate, trebuie să achiziţioneze permanent noi programe antivirus.

Pentru a se face diferenţa dintre pericolele reale şi cele generate şi întreţinute artificial, voi arăta amănunţit pericolele actuale, ca şi pe cele potenţiale. Nimic de zis, riscurile descrise mai jos şi discutate foarte aprins în presă există. Sunt însă pericole mai mult de natură academică decât reale.

1. Cabir, viermele pentru mobile

Prin definiţie, Cabir este un vierme, deoarece se reproduce şi se transmite mai departe, însă nici nu poate fi comparat alţi viruşi de pe Internet. Atacă exclusiv telefoane mobile cu sistem de operare Symbian şi încearcă să se transmită mai departe via bluetooth. Acest lucru li se poate întâmpla doar aparatelor a căror interfaţă bluetooth este activată şi deschisă comunicaţiei. În plus, recepţia viermelui trebuie acceptată separat. O dată intrat în sistemul de operare, Cabir caută în fundal după alte aparate bluetooth (inclusiv scannere şi imprimante) şi se transferă mai departe pe primul aparat găsit.

Se poate evita o astfel de situaţie dacă nu se accepta nici un fel de date care vor să se transfere neanunţate pe mobilul destinatarului. Chiar dacă expeditorul este cunoscut, este bine să cunoaştem dinainte conţinutul pe care vrea să îl trimită. Dacă totuşi ajunge un astfel de mesaj pe un telefon, dezinstalarea lui este foarte uşoară, prin utilizarea instrucţiunilor prescrise în acest scop şi care pot fi găsite pe site-urile firmelor producătoare de programe antivirus.

2. Virusul Commwarrior

Un nou virus a început sa se propage prin intermediul mesajelor foto si audio transmise de pe telefoanele mobile, fiind primul de acest fel care ameninţă telefonia mobilă la nivel mondial, relatează Reuters.Virusul Commwarrior se multiplică prin transmiterea de mesaje multimedia persoanelor aflate in listele de contact ale telefoanelor mobile şi încearcă să facă acelaşi lucru prin conexiunile Bluetooth. Spre deosebire de viruşii de computer, care se răspândesc rapid prin Internet, viruşii de pe telefoanele mobile au fost limitaţi pana acum de tehnologia acestora. Cabir, primul virus de telefon mobil din lume, s-a propagat în numai 16 state, în decurs de 6 luni, folosind conexiunile Bluetooth. Commwarrior.încearcă să transmită mesaje multimedia (MMS) cu diferite denumiri telefoanelor care utilizeaza software-ul de operare al companiei Symbian, se arată într-un comunicat al producătorului de software de securitate Symantec.

Mesajul infectat primit invita utilizatorul sa execute fişierul atasat, sub pretextul că acesta conţine un joc 3D, o felicitare, un antivirus sau chiar clipuri pornografice. Deşi nu distruge telefonul sau datele de pe acesta, virusul are drept efect trimiterea masivă de MMS-uri, ceea ce duce la consumarea bateriilor şi la o factura telefonică pe măsură. Dacă acestui virus i se va ataşa o componentă distructivă, potenţialul său va fi cu adevărat periculos, în măsura în care extrem de puţini utilizatori de telefoane mobile avansate au instalat un antivirus pe acestea.

Dacă utilizatorul nu descarcă mesajul, virusul nu se răspândeşte. "Nu cred că acest virus va fi o mare problemă, dar este începutul unei noi ere", a declarat Mikko Hypponen, director la compania finlandeză de cercetari antivirus F-Secure. Acesta a adăugat că primele indicii arată că virusul provine din Rusia. Cel mai mare producător de telefoane mobile, care controlează 48% din Symbian, a apreciat că industria producătoare de telefoane mobile este pregatită sa facă faţă viruşilor şi poate învăţa din lumea computerelor personale.

3. Bluejacking

Aşa-numiţii bluejackers se distrează enorm trimiţând mesaje ascunse în numele aparatului expeditor, de genul „Salut, eşti victima unui bluejacking!” Ei caută prin împrejurimi aparate disponibile, ce au interfaţa activată şi sunt pregătiţi pentru recepţia de date. Dacă au descoperit unul, îi trimit acestuia o carte de vizită goală. La victimă apare numele aparatului – în acest caz, mesajul – înainte de a apărea textul „vrea să vă trimită o carte de vizită”. Bluejacking nu este atât de periculos, cât e de enervant.

Şi în acest caz, pentru a ne proteja, nu trebuie să acceptăm recepţia datelor, fie ele chiar şi cărţi de vizită, al căror expeditor nu-l cunoştem. Pentru a ocoli astfel de evenimente, ar trebui

dezactivat bluetooth-ul sau setat mobilul pe „invizibil”, permițând doar conectarea cu aparatele cunoscute.

4. Lipsuri bluetooth

Fără îndoială, pericolul reprezentat de lipsurile din securitatea firmware-urile telefoanelor mobile este real. La unele telefoane mai elaborate există posibilitatea de a prelua controlul asupra diferitelor funcții. Un pericol real îl presupun şi fisurile din software-ul de control, descoperite nu de mult de firma Integralis. Acestora li se adaugă aşa-numitul „Bluesnarf” şi agresiunile „Chaos Attack”. În ambele cazuri sunt folosite punctele slabe ale software-ului, pentru a prelua controlul asupra mobilului prin intermediul diferitelor comenzi. În cazul bluesnarfing-ului, se citesc informații de genul contactelor din agendă, informații din calendar sau numărul de serie al mobilului, fără ştirea posesorului. În cazul „Chaos Attack”, atacatorul poate atinge chiar controlul asupra unor funcții ale telefonului prin supraaglomerarea buffer-ului (buffer overflow), ajungând să scrie SMS-uri, să realizeze apeluri, să scrie informații pe SIM sau în memoria agendei.

Totuşi, nici această situație nu este foarte îngrijorătoare, deoarece probabilitatea de a cădea victimă unui asemenea atac este foarte scăzută. În plus, pentru un atac de succes, trebuie atinse nişte condiții ideale: în timp ce mobilele cu bluetooth au o rază de acțiune de maxim 10 metri, hacker-ul trebuie să caute ceva vreme pentru a găsi un telefon cu interfața bluetooth activată, care să se mai şi afle în modul de lucru „vizibil”. Apoi, chiar dacă se confirmă toate aceste şanse, potențiala victimă nu trebuie să iasă din raza de acțiune a hacker-ului pe toată durata desfăşurării atacului. Atacuri efective în afara condițiilor de laborator sunt puțin viabile. Mai important, atacurile pot fi evitate prin intermediul unor metode foarte simple.

Cel mai la îndemână mod de a protejare este dezactivarea modulului bluetooth. Dacă este utilizat un headset radio pentru a telefona, în meniul bluetooth trebuie trecut pe modul de funcționare „invizibil”, fiind astfel indisponibil pentru aparatele străine. Aparatele cu care eşti deja cuplat, de exemplu un headset, vor realiza conexiunea chiar şi fără „să vadă” efectiv aparatul. Trebuiesc şterse pairing-urile de care nu mai ai nevoie de pe listă şi controlat în mod regulat dacă nu a apărut un aparat străin în lista aparatelor agreate. Multe telefoane mobile oferă posibilitatea de a realiza legături doar după acceptul uneia sau al ambelor părți. Este necesar folosirea acestor posibilități, chiar dacă e mai obositor. În general, trebuie acceptate doar conexiuni de la persoane cunoscute.

5. Denial of Service

Atacurile Denial of Service sunt deja bine cunoscute din lumea calculatoarelor. Prin intermediul mai multor calculatoare, serverele sau site-urile Web ale firmelor sunt invadate de cantități de date atât de mari, încât acestea nu le mai pot prelucra şi cedează. Procedeul funcționează la fel şi în cazul telefoanelor mobile. Atacuri via SMS, bluetooth, MMS - există mai multe posibilități de a îngenunchea un terminal mobil de pe un calculator sau de pe un alt telefon mobil. Însă Denial of Service (DoS) nu este realmente vătămător, ci doar extrem de enervant. Victimele trebuie doar să-şi repornească telefoanele mobile, prin îndepărtarea acumulatorului şi reintroducerea lui. În afară de asta, şi pentru hacker e destul de obositor să atace acelaşi mobil vreme îndelungată, aşa că astfel de scenarii nu ți se vor întâmpla prea des.

O altă metodă de a imobiliza telefonul mobil constă în trimiterea unui SMS ce conține un anumit şir de numere. Acest mesaj e menit să profite de micile erori din firmware-ul telefoanelor, pentru a crea un buffer overflow. Prin acelaşi truc (scoaterea acumulatorului şi punerea lui la loc) se poate rezolva şi această problemă.

Împotriva DoS nu te prea poți apăra, deoarece teoretic orice serviciu al provider-ului de servicii mobile poate fi folosit pentru un astfel de atac. Pentru a evita apariția unor probleme mai mari, pur şi simplu reporneşte mobilul.

6. Mesaje-farse mobile

Farsele sunt mesaje false, răspândite prin e-mail, menite să declanşeze panică sau isterie în masă. De cele mai multe ori, ele se referă la viruşi cunoscuți din lumea calculatoarelor sau la oameni care cer ajutor, ajutor ce poate fi dat prin simpla trimitere a unui e-mail. Astfel de bancuri proaste sunt folosite şi sub pretextul viruşilor pentru mobil: mesajul spune că firma XY oferă gratuit telefoane mobile, cu condiția ca tu să le scrii un e-mail. Aceste mesaje nu-ți aduc nici un prejudiciu real, fiind

doar umplutură pentru căsuţele poştale, ce au darul de a băga nesiguranţa în mintea utilizatorilor ce le primesc. Panica este uneori destul de mare, deoarece conţinutul mesajelor poate fi abil redactat. Sunt posibile, chiar dacă încă nu s-au consemnat, recepţionări a unor astfel de mesaje-farse prin SMS direct pe mobil.

7. Dampig, troianul pentru telefoane mobile

Autorii de viruşi au creat un nou troian capabil să infecteze telefoanele mobile smaprtphone din seria Symbian Series 60. Dampig-A, descoperit la 4 martie, îşi păcăleşte victimele pozând drept o copie piratată a aplicaţiei FSCaller, dezvoltată de SymbianWare.

Troianul dezactivează o serie de aplicaţii integrate în smartphone şi încearcă să instaleze în acesta variante ale viermelui Cabir. „Nici una din variantele de Cabir instalate nu se execută automat, dar unele dintre aplicaţiile care sunt înlocuite cu executabile Cabir sunt la un moment dat utilizate de posesorul telefonului şi astfel executate chiar de acesta", a arătat compania de securitate informatică F-Secure.

Eforturi pentru izolare

Contracararea acestor tentative de infectare a dispozitivelor mobile a devenit una dintre preocupările firmelor de securitate din domeniu. „În orice caz, prin informaţii sofisticate si analize, IBM poate identifica şi înţelege acum multe dintre aceste riscuri. În plus, afacerile si clienţii pot utiliza aceste informaţii nu numai pentru anticiparea riscurilor de securitate, dar şi pentru a evita noile tipuri de atacuri din 2005", consideră Stuart McIrvine, director al Strategiei de Securitate IBM.

Şi companiile care creează soluţii antivirus au inceput să caute metode de contracarare a viruşilor din această categorie. „Lucrăm în prezent la un antivirus pentru Symbian", spune Patrick Vicol, analist virusi Bit Defender. Rămâne de văzut dacă viruşii creaţi pentru dispozitivele mobile vor deveni mai periculoşi, şi în ce măsură acţiunile acestora vor fi contracarate la timp.

Bibliografie:

1. Heywood D., - „Secrete Windows NT Server 4", Editura Teora, Bucureşti, 1998, pag. 773
2. http://news.softpedia.com
3. www.chip.ro/
4. www.bluejackq.com/
5. www.f-secure.com