Viermele “CodeRed”

Mihai Budiu — mailto:mihaib+@cs.cmu.edu
http://www.cs.cmu.edu/~mihaib/

august 2001

Subiect: cel mai eficace vierme electronic care a infectat Internetul

Cunoştinţe necesare: cunoştinţe elementare despre funcţionarea calculatoarelor

Cuvinte cheie: infecţie, vierme, virus, Microsoft IIS

Cuprins

1 Cu 13 ani în urmă

Pe 2 noiembrie 1988 unele din calculatoarele cuplate la reţeaua numită Internet, care lega o parte dintre marile universităţi şi centre de cercetare americane, au început să exhibe simptome ciudate. Calculatoarele executau tot felul de programe, compilau surse şi comunicau cu alte calculatoare din reţea, fără ca cineva să fi iniţiat aceste activităţi. Prima alarmă a fost pornită la universitatea Stanford, la ora 9 seara (ora coastei de est a Statelor Unite), care afirma că majoritatea maşinilor Unix din campus (în număr de vreo 2500) erau infectate de un virus care pornise de la MIT. La ora 10 seara programatorii de la MIT au descoperit şi ei o activitate suspicioasă şi au încercat să reboot-eze calculatoarele, crezînd că e vorba de un program care a luat-o razna. Cînd au observat însă că, nu mult timp după repornire, calculatoarele re-începeau acelaşi lanţ de activităţi bizare, au realizat că ceva mai serios se află la mijloc.

În curînd mesaje de e-mail schimbate cu colegi de la alte universităţi le-au revelat că atacul era universal: calculatoare din toată America sufereau de aceleaşi simptome. Au urmat apoi două nopţi albe şi muncă în foc continuu în care hacker-ii încercau să înţeleagă în ce fel funcţionează noul virus care le ataca calculatoarele. La fel ca şi cei biologici, care forţează celulele organismului gazdă să-i multiplice, viruşii informatici de obicei călătoresc pe "spinarea" altor programe. Programul cel nou era însă autonom; ca atare a fost botezat "vierme": era un organism de sine-stătător, capabil să se multiplice şi să atace de la sine alte calculatoare.

Cercetătorii au atacat viermele prin mai multe metode:

- au început să-l dezasambleze şi să descifreze instrucţiunile din care era compus;
- au creat maşini-capcană pe care să le infecteze, care înregistrau o mulţime de detalii despre ceea ce se petrecea cu ele însele (creau "log"-uri);
- au creat maşini-mutant pe care le paralizau parţial, pentru a descoperi care sunt serviciile de care viermele are nevoie pentru a se putea multiplica.

Viermele acesta era deosebit de virulent şi complicat, atacînd staţii de lucru Sun şi VAX care rulau sistemul de operare Unix de la Berkeley. Viermele folosea mai multe metode de propagare, exploatînd mai multe slăbiciuni în configurarea calculatoarelor şi implementarea programelor:

- Întîi încerca să se transfere între calculatoare pe care acelaşi utilizator avea conturi diferite şi între care utilizatorul îşi configurase acces fără parole (folosind fişierele `.rhosts`);
- Dacă nu reuşea folosind acest mecanism, încerca să folosească o slăbiciune din programul `sendmail`, care şi la ora actuală este cel mai folosind program pentru procesarea poştei electronice. Pe multe calculatoare `sendmail` era instalat compilat cu o configuraţie de depanare, care permitea executarea unor comenzi de la distanţă;
- În fine, viermele exploata un bug din implementarea programului `finger`, care este folosit în mod normal pentru a vedea cine lucrează pe un calculator la distanţă. Viermele exploata pentru prima oară un tip de bug numit "buffer overflow": viermele trimitea programului `fingerd`, care primeşte întrebări despre utilizatori prin reţea, un nume de utilizator foarte lung, care depăşea memoria alocată pentru recepţia mesajului. Numele era atît de lung încît scria gunoi peste stiva programului şi modifica valoarea salvată a registrului PC (program counter, care indică instrucţiunea următoare). Aceasta cauza un salt la o adresă dinainte stabilită, aflată în numele foarte lung, unde viermele conţinea cod care prelua controlul.
- Odată instalat pe un calculator, viermele încerca să decripteze unele din parolele utilizatorilor folosind un dicţionar de parole frecvent folosite, pentru a pune mîna pe noi conturi din care să re-atace folosind prima metodă;
- Viermele se propaga în două etape pe un nou calculator pe care-l infecta: întîi trimitea un scurt program scris în C, care era compilat pe maşina locală, care apoi aducea şi restul viermelui, care consta în module pre-compilate pentru Sun şi VAX;
- În interiorul viermelui toate şirurile de caractere (inclusiv comenzile pe care viermele le lansează în execuţie şi dicţionarul de parole inclus) erau "ascunse" (fiecare caracter este suprapus cu un *sau exclusiv* (XOR) cu valoarea hexazecimală 81).

Viermele nu efectua acţiuni distructive, cum ar fi ştergerea de fişiere sau instalarea de conturi ascunse: singurul efect negativ provenea din faptul că maşinile erau infectate în mod repetat, şi curînd nu făceau altceva decît să execute copii ale viermelui.

Cercetări ulterioare au relevat faptul că viermele fusese creat şi lansat de un student la doctorat al universităţii Cornell, pe nume Robert Tappan Morris. În mod oarecum ironic, Morris este fiul unui alt Robert Morris, care era pe vremea aceea cercetător la National Security Agency, organizaţia guvernului americană însărcinată cu criptologia.

Pentru propagarea viermelui, Robert Morris a fost condamnat la trei ani de închisoare cu suspendare, 10000 de dolari amendă şi 400 de ore de muncă în serviciul comunităţii. După terminarea sentinţei Robert Morris a terminat doctoratul la universitatea Harvard şi începînd din 1999 este profesor la universitatea MIT, lucrînd în domeniul reţelelor de calculatoare. Să nu faceţi cumva greşeala să credeţi că Morris a avut aceste succese ulterioare datorită păţaniei cu viermele: el a reuşit să-şi "repare" cariera *în pofida* istoriei cu viermele, pentru că este un ins foarte capabil şi inteligent. În prezent refuză să vorbească despre vierme sau să facă cercetare în securitatea calculatoarelor.

O mulţime de rapoarte au descris aceste evenimente în detaliu şi au discutat problema securităţii în Internet imediat după aceste evenimente. Cu toate acestea, nimic nu s-a schimbat...

2 O problema în serverul de web de la Microsoft

Pe data de 18 iunie 2001 compania Eeye Digital Systems a publicat informaţii despre o problemă de securitate în serverul de web al companiei Microsoft, numit IIS. Bug-ul este de exact aceeaşi natură ca şi în urmă cu 13 ani: buffer overflow. Microsoft a emis o corecţie pentru această problemă la scurt timp după aceea. La ora actuală se estimează că există aproximativ două milioane de calculatoare care rulează acest program, care vine instalat automat cu Windows NT şi Windows 2000. Multe persoane probabil că execută acest program fără a şti măcar de existenţa lui.

Pe data de 12 iulie a fost semnalată pentru prima oară prezenţa unui vierme care exploata această slăbiciune. Această primă variantă a viermelui a fost denumită CodeRed versiunea 1; numele provine de la sucul "Code Red" care conţine un procent ridicat de cafeină, şi care i-a ţinut treji pe cercetătorii care atacau viermele cu aceleaşi arme ca în urmă cu 13 ani.

Viermele funcţionează în două etape:

- Între datele de 1 şi 19 ale lunii, viermele e în faza de infecţie, şi atacă noi calculatoare ale căror adrese le generează aleator, pentru a se multiplica;

- Pe data de 20 a fiecărei luni, viermele lansează de pe toate maşinile infectate un atac de tip DoS (Denial of Service) asupra unui calculator de la Casa Albă, cu adresa `www1.whitehouse.gov`.

- În plus, viermele schimbă paginile de web ale serverului atacat adăugînd mesajul "Hăcuit de chinezi", însă numai dacă serverul e configurat să opereze în limba engleză. Nu există nici o indicaţie că viermele ar fi fost creat în China.

Versiunea 1 a viermelui s-a răspîndit foarte lent, din cauză că un vierme nou infectat folosea aceleaşi adrese generate aleator (pornea de la aceeaşi "sămînţă" (seed) în generarea numerelor aleatoare), şi ca atare încerca să infecteze mereu şi mereu aceleaşi calculatoare.

Pe data de 19 iulie, în jurul orei 10 dimineaţă a apărut o variantă mutant a viermelui, care folosea o sămînţă generată aleator. Această mică schimbare a avut un impact colosal: pînă la sfîrşitul zilei acesteia viermele a infectat peste 400000 (patru sute de mii) de maşini! Probabil că ar fi infectat şi mai multe dacă nu ar fi intrat în faza a doua, care începea pe data de 20 a lunii.

Din fericire viermele verifică existenţa adresei atacate; pentru a preveni diluviul, administratorii de la Casa Albă au dezafectat serverul care era ţinta atacului distribuit. Dacă 400000 de calculatoare din toată lumea lansează un atac simultan în Internet, aceasta poate avea efecte dramatice asupra traficului.

Între timp mass-media a făcut o publicitate enormă virusului; astfel mulţi administratori de sistem au aflat de existentă lui şi au aplicat corecţiile de la Microsoft. Cu toate acesta, există în continuare un mare număr de calculatoare vulnerabile.

Pe 4 august a apărut un nou vierme, complet diferit, dar care conţine textul "CodeRed2". Acest vierme exploatează aceeaşi slăbiciune, dar odată instalat face ravagii pe calculatorul infectat, instalînd conturi ascunse pentru administratori care pot fi apoi folosite de la distanţă. În plus, acest vierme are un algoritm special prin care adesea selectează şi atacă în mod special calculatoarele din aceeaşi reţea cu victima.

La ora la care scriu acest articol (pe 27 august) a fost anunţată o a treia mutaţie a viermelui. Ţinînd cont de numărul uriaş de victime şi de probabilitatea practic nulă ca toate să fie peticite, e foarte probabil că acest vierme va continua să existe în Internet încă foarte multă vreme.

3 Legea logistică

Figura 1 arată numărul de calculatoare infectate ca funcţie de timp. Axa orizontală este ora iar axa verticală indică numărul estimat de calculatoare infectate. Am descris metoda prin care se poate estima numărul de calculatoare infectate în articolul meu din NET Report din luna iulie. Acest număr se poate estima numărînd atacurile care vin într-o anumită porţiune din reţea de la serverele infectate (această tehnică a fost numită în articolul meu anterior "împrăştiere"; fenomenul în acest caz este puţin diferit, dar mijloacele folosite pentru estimare sunt aceleaşi).

Curba din figura 1 are o formă numită "sigmoidă", avînd două zone distincte:

(a) O zonă în care infecţia urmează o curbă exponenţială; începutul este lent, rata de infecţie fiind scăzută, dar după ce un număr suficient de mare de calculatoare este infectat, viteza cu care infecţia se răspîndeşte este uluitoare.

(b) O zonă în care infecţia se plafonează la o valoare limită. În cazul acestui vierme, platoul a fost atins pentru că viermele era pre-programat să-şi oprească multiplicarea la ora 24.

Chiar dacă viermele nu este pre-programat să se oprească, trebuie să ne aşteptăm ca viteza de infecţie să urmărească o astfel de curbă. Similitudinea cu un organism biologic este din nou frapantă: zoologii care studiază evoluţia unei populaţii de animale au descoperit această lege de înmulţire cu mult timp în urmă, şi i-au dat şi un nume, "legea logistică".

Legea logistică poate fi descrisă printr-o formulă aparent complicată, dar care la o analiză atentă este foarte naturală:

$$\frac{dN}{dt} = rN\left(\frac{K-N}{K}\right).$$

Simbolurile din această din această formulă reprezintă:

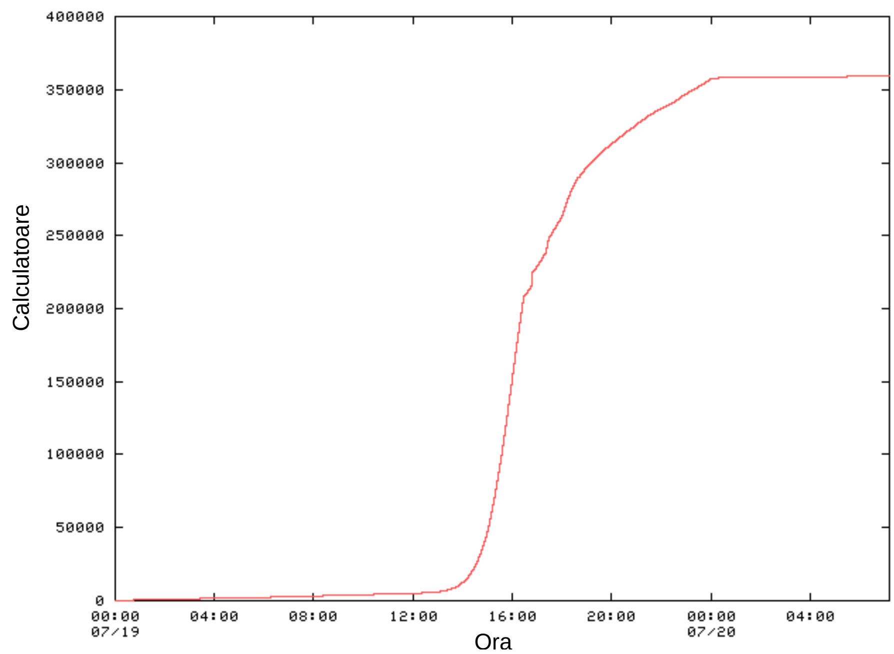

Figura 1: *Multiplicarea viermelui codeRed, versiunea a doua, pe data de 19 iulie 2001. Ora este cea a meridianului Greenwich. Această figură este extrasă din pagina de web de la CAIDA,* `http://www.caida.org/analysis/security/code-red/gifs/cumulative-ts.gif`.

- N este numărul de noduri infectate, o funcţie de timp t;
- r este "rata infecţiei": numărul de calculatoare pe care un ins infectat le infectează la rîndul lui într-o unitate de timp;
- K este o valoare numită de zoologi "capacitatea mediului": numărul de indivizi care pot fi suportaţi de resursele ecologice. În cazul nostru, K este populaţia totală de calculatoare care rulează programul defect.

Putem recunoaşte în legea logistică cele două părţi ale sigmoidei:

(a) Zona iniţială, în care N este mic comparat cu K. În această zonă fracţia dintre paranteze este aproape 1, şi legea devine $dN/dt = rN$, ceea ce prin integrare în raport cu timpul devine $N(t) = r^t$, deci o curbă exponenţială. Explicaţia este naturală: în prima generaţie avem un calculator, în a doua el va infecta r calculatoare, în a treia fiecare va infecta alte r, deci vom avea r^2, apoi r^3, etc.

(b) Cînd numărul de calculatoare infectate N devine comparabil cu populaţia K, tentativele de infecţie nu vor mai fi la fel de eficace: mai multe calculatoare diferite vor infecta aceeaşi victimă, deci generaţia curentă va creşte de mai puţin de r ori[1]. La limită, cînd toate

[1] Mai exact, probabilitatea ca un mesaj de infecţie să ajungă la un calculator "curat" este raportul dintre numărul de calculatoare ne-infectate $K - N$ şi numărul total K.

calculatoarele sunt infectate ($K = N$), fracţia devine $(K - N)/K = 0$, deci $dN/dt = 0$, deci populaţia nu mai creşte.

Ceea ce este înspăimîntător este viteza cu care infecţia s-a propagat: în doar 24 de ore infecţia a acoperit aproape jumătate de milion de calculatoare!

3.1 Calculatoare vulnerabile

Viermele CodeRed s-a bucurat de o publicitate enormă în presă: aproape că nu există ziar sau canal de televiziune care să nu fi menţionat viermele. Ca atare informaţia despre atac s-a propagat destul de bine şi a atins multă lume prin multe canale. Ne aşteptăm deci ca foarte mulţi dintre administratorii de sistem să fi luat măsuri aplicînd "peticele" de la Microsoft care corectează problemele din IIS.

CAIDA monitorizează şi numărul de calculatoare peticite, folosind o eşantionare statistică: dintre calculatoarele infectate iniţial, CAIDA alege la întîmplare cîteva şi trimite nişte cereri prin care poate afla dacă peticele au fost aplicate. Multe din calculatoarele infectate iniţial nu răspund la aceste pachete de test, probabil pentru că unele dintre ele nu au adrese IP fixe. Dintre calculatoarele testate însă, graficul din figura 2 arată cîte au fost peticite.

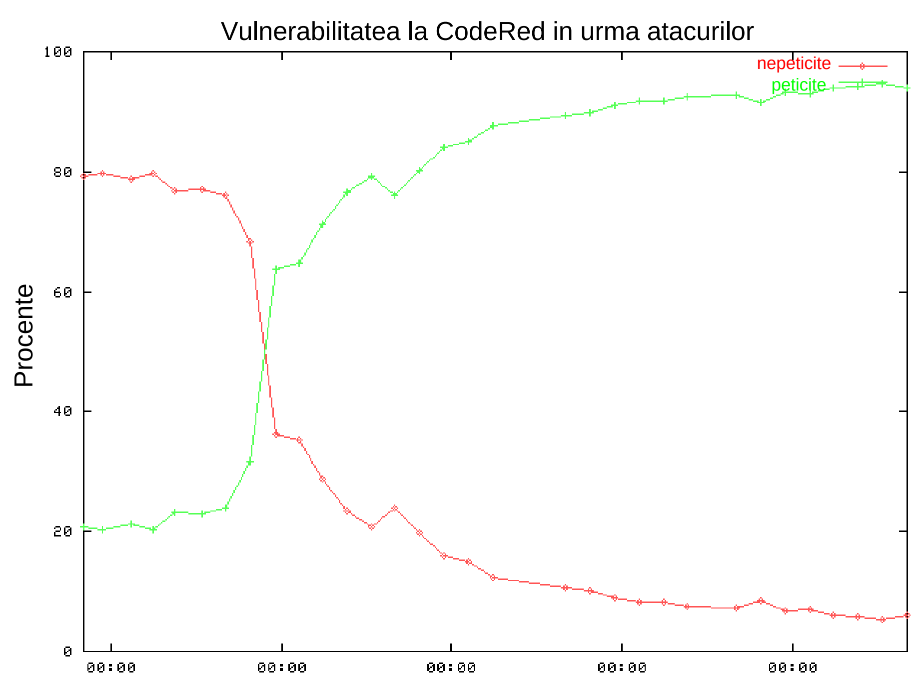

Figura 2: *Procentul estimat de calculatoare infectate care au aplicat peticele (patches) de la Microsoft în urma propagării viermelui. Acest grafic poate fi obţinut în timp real de la* `http://worm-security-survey.caida.org/patching.gif`.

4 Concluzii

Din acest text putem extrage două concluzii îngrijorătoare:

- Posibilitatea unui atac distructiv pe Internet la scală planetară nu mai este discutabilă, ci este o certitudine. În viitorul apropiat vom avea de a face cu atacuri mult mai periculoase, la o scară nemaiîntîlnită. În ce măsură Internetul va rezista acestora rămîne de văzut.
- Comunitatea programatorilor nu a învăţat mare lucru în ultimii 13 ani în privinţa securităţii informatice: aceleaşi tehnici pentru construit viruşi şi viermi funcţionează la fel de bine. Deşi aceste probleme sunt foarte bine înţelese, şi există o mulţime de soluţii parţiale propuse, ele nu sunt implementate în practică.

5 Alte surse de informaţie

- Un site de web dedicat primului vierme din Internet, lansat de Robert Morris de la universitatea Cornell în noiembrie 1988: `http://www.worm.net`. Acest site conţine codul sursă complet al viermelui.
- Un articol despre "disecţia" viermelui Morris făcută în timp real de o echipă de la MIT: "Cu Microscop şi Pensetă": `http://www.worm.net/worm-chronology.html`.
- Pagina de web a autorul primului vierme Internet, Robert Morris, acum profesor la universitatea MIT: `http://www.pdos.lcs.mit.edu/~rtm`.
- Site-ul de web al companiei Eeye Digital Systems, care a publicat prima slăbiciunile pe care este bazat CodeRed, şi care a lucrat la înţelegerea mecanismelor prin care CodeRed funcţionează: `http://www.eeye.com`.
- Analiza şi vizualizarea viermelui CodeRed făcute de organizaţia CAIDA (Cooperative Association for Internet Data Analysis), asociată cu centrul de supercalculatoare al universităţii din California, San Diego: `http://www.caida.org/analysis/security/code-red`. Acest site continuă să monitorizeze infecţia şi numărul de calculatoare care au fost peticite împotriva atacului.
- Articolul meu din NET Report despre atacuri de tip "Denial of Service" din iulie 2001: `http://www.cs.cmu.edu/~mihaib/articles/articles.html#ddos`.
- Cît de rapidă poate fi răspîndirea unui vierme? Un articol despre un vierme ipotetic numit Warhol, care poate acoperi întreaga planetă în 15 minute (poate infecta 99% din toate calculatoarele vulnerabile): `http://www.cs.berkeley.edu/~nweaver/warhol.html`
- Peticele de la Microsoft pentru IIS: `http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/topics/codealrt.asp`.
- O sculă de la Microsoft care dezinfectează calculatoarele infectate cu CodeRedII: `http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31878.`.