Nu vă lăsați PC-ul să fie păcălit de 1 aprilie!

» Pe 1 aprilie, calculatorul administrator al rețelei de PC-uri care rulează Windows și au fost infectate până acum de viermele Conficker este programat să preia controlul tuturor acestora.

» Modul în care s-a răspândit acest virus i-a determinat pe cercetători să afirme că ceea ce urmează să se întâmple este puțin probabil să fie o păcăleală.

Dina Rădulescu
REDACTOR

ULTIMA VARIANTĂ A VIERMELUI CONFICKER e pe punctul să lanseze un atac major, avertizează toți marii jucători din industria de securitate informatică. Conficker C sau Downadup este codificat pentru a se activa pe data de 1 aprilie 2009.

Cele mai luminate minți din industria IT lucrează în aceste zile pentru a reduce impactul virusului cât de mult se poate, însă sunt deja peste 10 milioane de calculatoare care au fost infectate și care vor asculta comenzile primite de la distanță. „Deși infestate, aceste PC-uri nu manifestă multe simptome, dar pe data de 1 aprilie un calculator administrator este programat pentru a prelua controlul asupra lor", a declarat Don DeBolt, directorul de cercetare a amenințărilor de la Computer Associates.

Motivul? Doar speculații

Nici până acum, experții în securitatea computerelor nu au o idee precisă asupra naturii acestor comenzi.

Programul ar putea să șteargă toate fișierele dintr-un calculator personal sau să utilizeze aceste calculatoare zoombie pentru a închide site-uri Web sau pentru a monitoriza și colecta informații confidențiale, cum ar fi parole sau informații despre conturi bancare.

Unii specialiști susțin că cel mai probabil virusul ar putea încerca să determine utilizatorii de calculatoare să cumpere software-uri falsificate sau să își cheltuiască banii pe alte produse contrafăcute. Alții sunt mult mai îngrijorați și alimentează speculațiile conform cărora acțiunea se va materializa într-un atac devastator asupra însăși infrastructurii internetului. „Principalul scop al autorilor acestui vierme este cel de a construi și consolida o rețea de clone de proporții fără precedent care să poată fi exploatată pentru un atac masiv împotriva infrastructurii internet sau pentru spionaj la scară largă", a declarat Juraj Malcho, coordonatorul ESET Virus Lab.

Ușor de verificat

Dacă primii au dreptate, atunci noi, ca simplii utilizatori, știm ce avem de făcut: ne abținem să dăm imediat click pe orice link primit de oriunde (e-mail-uri nesolicitate sau mesaje pe Messenger, cu link-uri ciudate, primite chiar și de la prieteni). E mai bine să nu luăm în considerare mail-urile care nu ne privesc sau să întrebăm expeditorul – dacă îl cunoaștem – care este contextul expedierii.

Dar dacă este vorba de ceva mai grav? Cel mai bine ar fi să ne verificăm PC-ul dacă este „înregimentat" în armata zoombie.

DeBolt afirmă că virusul pătrunde adânc într-un calculator, acolo unde este dificil de descoperit. Programul împiedică Windows-ul să realizeze update-urile automate, care ar putea preveni daunele cauzate de acest virus.

De aceea, o metodă rapidă de a afla care este starea calculatorului dumneavoastră este de a verifica dacă există update-uri ale Windows-ului în luna martie. Dacă acestea există, cel mai probabil calculatorul dvs. nu a fost infestat. ▮

CE SIMPTOME SUNT

Virusul, programat să se răspândească atât prin internet, dar și prin intermediul dispozitivelor de stocare mobile (stick-uri USB) execută următoarele modificări asupra calculatoarelor infectate:

» blochează toate instrumentele care au legătură cu securitatea sistemului de operare, modificând înregistrările DNS

» blochează sau dezactivează aplicațiile de securitate

» are abilitatea de a comunica în interiorul rețelelor peer-to-peer (P2P)

» începând din 1 aprilie 2009 va verifica pentru instrucțiuni de pe 50.000 de domenii de internet pe zi.

CUM VERIFICĂM

Dacă nu aveți ultimul update de Windows și vă temeți că ați putea avea PC-ul infectat, puteți să vizitați paginile http://safety.live.com sau http://bdtools.net.
„Infecția cu Downadup poate fi verificată ușor, spune Vlad Vâlceanu, Head of Antispam, BitDefender. Dacă puteți accesa www.google.com http://www.google.com, dar nu puteți accesa site-uri de securitate, cum ar fi www.microsoft.com http://www.microsoft.com, www.bitdefender.com http://www.bitdefender.com –, deși mai demult puteați să faceți acest lucru, sunt șanse maxime să fiți infectați cu Downadup. Virusul blochează serviciul de Windows Update, precum și accesul la site-uri de securitate.

CUM DEZINFECTĂM

Pentru a scăpa de virus, puteți să intrați pe http://bdtools.net sau http://safety.live.com să descărcați și rulați tool-ul gratuit de dezinfecție. Dacă e nevoie, restartați calculatorul. Veți avea din nou acces la Internet.
Atenție mare: acest tool nu vă protejează de reinfecție! „Dacă faceți parte dintr-o rețea infectată, vă veți reinfecta, avertizează Vlad Vâlceanu. Pentru a fi protejat complet, trebuie să folosiți o soluție antivirus bună și să vă actualizați sistemul de operare folosind Windows Update".
De aceea, și persoanele care utilizează un software de antivirus ar trebui să verifice dacă au primit ultimele update-uri, deoarece este posibil ca și aceste sisteme să fi fost afectate de Conficker C.