G Data press release 2012

Dorifel, viermele criptat, ataca

Clientii G Data sunt protejati impotriva acestui program malware periculos

Bucuresti (Romania) 20.08.2012 – Programul malware numit Dorifel, care cripteaza fisiere Word si Excel pe computerele infectate, circula pe Internet. Viermele aparut pentru prima data in Olanda este acum raspandit si in Germania, USA, Danemarca si Filipine. Se estimeaza ca a infectat mii de computere in toata lumea si exista riscul ca acesta sa se raspandeasca si in alte tari din Europa, printre care si Romania. Dorifel a fost initial introdus in computere prin atasamente de email infectate. Botnetul Tatanga, folosit de infractori si pentru a sustrage date bancare, este cel mai probabil responsabil de trimiterea acestor emailuri. In consecinta, atacatorilor le este la indemana sa foloseasca Dorifel pentru a penetra si a sustrage informatii ale utilizatorilor de pe conturi de online banking. Clientii G Data nu au niciun motiv sa se teama pentru siguranta datelor personale deoarece sunt deja protejati impotriva Dorifel, datorita eficientei tehnologiilor de securitate "Made in Germany".

"Multumita tehnologiilor proactive si a metodei eficiente de scanare, DoubleScan, integrate in solutiile noastre de securitate, clientii nostri sunt protejati de la bun inceput impotriva acestei amenintari," explica Ralf Benzmüller, sef al G Data Security Labs.

Ponturi de protectie impotriva Dorifel oferite de G Data:

- Utilizatorii ar trebui sa foloseasca o solutie cuprinzatoare de securitate care monitorizeaza permanent traficul http. Aceasta ar trebui sa asigure computerelor protectie eficienta impotriva programelor de descarcari automate efectuate fara consimtamantul sau chiar fara stirea utilizatorului (Drive-by Downloads). Este recomandat si un filtru anti-spam care sa opreasca emailurile nedorite.

- Sistemele de operare instalate, browserele si solutiile de securitate ar trebui sa fie mentinute cu updateuri la zi, pentru a acoperi in cel mai scurt timp bresele de securitate existente.

- Emailurile primite de la expeditori necunoscuti ar trebui sterse fara a fi deschise. Atasamentele, precum carduri de felicitari online sau videoclipuri, nu ar trebui deschise, iar link-urile incluse in emailuri nu ar trebui accesate.