G Data press release 2011

G Data neutralizeaza troianul federal

Specialistul german in securitate pe Internet face lumina in cazul descoperirii Chaos Computer Club

Bucuresti, 18 Octombrie 2011

G Data anunta ca solutia sa de securitate a detectat si neutralizat troianul federal descoperit si publicat de Chaos Computer Club (CCC). In aceste zile, Europa a asistat la o dezbatere apriga despre un troian folosit de mai multe districte din Germania pentru a spiona persoane suspecte. G Data isi mentine pozitia ferma atunci cand afirma ca nu agreaza folosirea unor astfel de metode in scopul spionarii persoanelor civile. Expertii G Data Security Labs nu se asteapta la o raspandire necontrolata a acestui malware.

"Am analizat software-ul la care se face referire ca Federal Trojan si putem confirma ca acesta a fost detectat de solutia noastra de securitate. Putem afirma cu siguranta ca utilizatorii solutiilor noastre nu sunt in pericol de a se fi infectat cu acest malware," spune Ralf Benzmüller, Head of G Data Security Labs.

Conform expertilor G Data, cifrele exacte ale raspandirii acestui nou troian sunt greu de aflat. Bazandu-se pe cifrele din acest weekend emise de propriul program, Malware Information Initiative, G Data nu a gasit evidente care sa sugereze ca troianul a fost foarte raspandit. Toate infectarile de pana acum inregistrate de G Data au fost stopate inainte ca troianul sa fie salvat sau activat.

Intrebari si raspunsuri ale expertilor G Data cu privire la troianul federal:

Q: Au detectat solutiile G Data acest troian?
A: Da, acesta a fost detectat ca Backdoor.R2D2.a

Q: Care sunt riscurile la care sunt expusi cei infectati?
A: Pe langa faptul ca multe date pot fi colectate si trimise remote catre o terta parte, troianul poate incarca aplicatii care pot fi exploatate de infractori pentru a instala si rula alte programe malware pe sistemul infectat

Q: Cum este afectat detinatorul datelor?
A: Comunicatia cu serverul de comanda si control al troianului este slab securizata. Asta face posibil ca tot felul de date sa poata fi trimise catre server, folosind o adresa pretinsa a fi originala. Toate informatiile colectate de autoritati sunt astfel usor de contestat.

-###-