G Data press release 2015

Programul spyware Casper foloseste o bresa de securitate pentru a accesa computerele

Este al treilea program malware conectat la documentele serviciilor de informatii canadiene.

Bucuresti (Romania) 10.03.2015

Un alt membru al familiei Cartoon malware - Casper - a fost descoperit, pe urmele pasilor lui Babar si EvilBunny. Expertii in securitate de la G DATA cred ca malware-ul Casper este succesorul programelor Babar si EvilBunny si a fost dezvoltat de aceleasi programatori - potential cu conexiuni la serviciul de informatii francez. Informatiile initiale despre malware au fost extrase din documentele provenite de la serviciile secrete canadiane, CSEC, care au iesit la lumina ca parte a dezvaluirilor lui Snowden. Cu toate acestea, Casper prezinta diferente interesante fata de predecesorii sai. Malware-ul este conceput a fi modular, astfel incat software-ul necesar pentru obiectiv sa poate fi descarcat, si include o tactica pentru combaterea solutiilor de securitate. Babar era deja capabil sa identifice solutia de securitate instalata pe sistem, dar Casper face un pas inainte: pe langa identificarea solutiei antivirus poate initia diferite strategii pentru a fenta detectia. Analiza a aratat ca malware-ul Casper exploateaza o bresa de securitate (zero-day exploit) in Adobe Flash Player, pentru a accesa computerul. Malware-ul primeste comenzi de la un site web inregistrat de Ministerul Sirian de Justitie, pe care cetatenii sirieni pot depune plangeri ale incalcarilor juridice.

Puteti gasi informatii detaliate despre Casper in G DATA SecurityBlog:
https://blog.gdatasoftware.com/blog/article/casper-the-newest-member-of-the-cartoon-malware-family.html

-###-