G Data press release 2014

G DATA sprijina BKA in lupta impotriva infractorilor cibernetici

Expertii in securitate din Germania ofera un instrument gratuit pentru eliminarea Dropperbot.

Bucuresti (Romania) 12.01.2015

Potrivit rapoartelor initiale, malware-ul Dropperbot a infectat 11.000 de computere din intreaga lume - aproximativ jumatate dintre acestea fiind localizate in Germania. Biroul Federal al Politiei Judiciare (BKA) a intervenit, a oprit botnet-ul si a intrerupt distributia acestuia. Malware-ul a fost distribuit pe Usenet in fisiere aparent inofensive si a fost instalat pe computer prin simpla deschidere a fisierului. Malware-ul fura date sensibile de pe conturi de retele sociale si date de acces pentru servicii online, intercepteaza intrarile de pe tastatura si face capturi de ecran. Aceste date sunt apoi transmise catre adrese predefinite. Acum, ca autorii au fost arestati, tot ce ramane de facut este curatarea computerelor. G DATA furnizeaza tuturor utilizatorilor un instrument gratuit pentru a detecta si elimina Dropperbot. Instrumentul functioneaza independent de orice software antivirus instalat. Solutiile de securitate G Data detecteaza malware-ul si protejeaza impotriva infectiei.

" Prin instrumentul Dropperbot Cleaner, oferim utilizatorilor un program independent pentru depistarea fisierele malware si dezinfectarea computerelor compromise," explica Ralf Benzmuller, seful G DATA SecurityLabs.

Tool-ul Dropperbot Cleaner de la G DATA

G DATA Dropperbot Cleaner detecteaza si elimina malware-ul, atat prin identificarea intrarilor autostart din registrii, precum si Dropperbot in sine, iar sistemul este apoi curatat. Cu toate acestea, pentru ca este posibil ca software suplimentar sa ramana pe sistem, expertii de securitate G Data recomanda o scanare completa a calculatorului folosind un program antivirus comprehensiv.

Cum a ajuns Dropperbot pe computere

Malware-ul era ascuns si a fost distribuit prin fisiere aparent inofensive pe Usenet, o platforma de partajare de date si fisiere. Fiind deghizat in mod adecvat, acesta consta in fisiere malware executabile care sunt descarcate pe computer dupa ce se da click pentru a le deschide. Utilizatorii care nu au permis afisarea extensiilor de fisier ".exe" au fost pacaliti de catre pictogramele folosite de autori.

Malware-ul suplimentar spioneaza utilizatorii

TRUST IN GERMAN SICHERHEIT

Expertii de la G Data SecurityLabs sunt constienti ca exista doua tipuri diferite de fisiere malware transferate de downloader pe computerele infectate. Ambele fisiere pot fi catalogate ca programe stealers, sarcina lor principala fiind de a sustrage date de pe dispozitivele infectate. Unul dintre programele stealers este disponibil pe forumuri subterane pentru aproximativ 35 ESD (aproximativ 30 EURO). Ambele fisiere malware pot citi datele de pe social media si servicii online. Programele stealers pot stoca, de asemenea, intrarile de pe tastatura si pot genera capturi de ecran. Datele colectate sunt apoi trimise de catre atacatori la adrese predefinite.

Instrumentul poate fi descarcat gratuit de pe link-ul: https://www.gdata.de/rdk/dl-de-dropperbotcleaner

Informatii detaliate sunt disponibile pe G DATA Security Blog:

https://blog.gdatasoftware.com/blog/article/bka-strikes-a-blow-against-botnet-operators.html