TRUST IN GERMAN SICHERHEIT

G Data press release 2014

G DATA: Uroburos compromite Ministerul de Externe din Belgia

Aceasta este prima informatie publicata referitoare la folosirea rootkit-ului impotriva unui stat european.

Bucuresti (Romania) 16.05.2014

Prezenta programului spyware Uroburos, care a fost descoperit de G DATA, in reteaua unui minister al unui stat UE, a fost dovedita pentru prima data. Saptamana trecuta a aparut un raport referitor la un atac cibernetic asupra Ministerului belgian de Externe. Jurnalistii de la ziarul belgian De Standaard au aflat dintr-o sursa apropiata de serviciile secrete ca programul de spionaj Uroburos a compromis reteaua institutiei guvernamentale. Expertii in securitate de la G DATA au emis atentionari in februarie 2014 despre acest program rootkit extrem de complex si avansat si au indicat potentialul pericol: "Uroburos este proiectat pentru a actiona in retele mari ce apartin companiilor private, autoritatilor statului, organizatiilor si institutelor de cercetare."

Ce s-a intamplat?

In weekend, Ministerul de Externe belgian a confirmat ca a avut loc un atac cibernetic asupra retelei informatice, iar "informatii si documente cu privire la criza din Ucraina" au parut a fi sustrase din retea, conform ministrului belgian de externe, Didier Reynders. Atacul pare a fi avut loc in cursul saptamanii trecute. Nimic nu este cunoscut despre protagonistii atacului, cu exceptia faptului ca ar vorbi limba rusa.

Informatiile publicate duc catre concluzia ca rootkit-ul Uroburos a fost utilizat in acest atac. Expertii G DATA au analizat programul spyware si au descoperit nivelul de complexitate tehnica al acestuia in februarie 2014.

Informatii de baza despre Uroburos

Rootkit-ul numit Uroburos, descoperit de G DATA, actioneaza autonom si se raspandeste independent in retelele infectate. Sunt atacate chiar si computerele care nu sunt conectate direct la Internet. In opinia G DATA, pentru a construi un astfel de program sunt necesare investitii substantiale in personal si infrastructura. Designul si nivelul ridicat de complexitate al malware-ului dau nastere, prin urmare, la ipoteza ca originile se trag dintr-un serviciu secret. Bazandu-se pe detaliile tehnice, precum nume de fisiere, criptare si comportament, s-a suspectat ca Uroburos ar putea proveni din aceeasi sursa care a lansat atacul cibernetic asupra SUA in 2008. Programul utilizat atunci s-a numit "Agent.BTZ".

Uroburos este un rootkit compus din doua dosare – un driver si un fisier de sistem virtual criptat. Atacatorii pot folosi acest malware pentru a prelua controlul asupra computerelor infec-

tate, pentru a executa orice cod de program si pentru a-si acoperi actiunile efectuate. Uroburos este totodata capabil sa sustraga date si sa inregistreze traficul de date din retea. Structura modulara le permite atacatorilor sa dezvolte malware-ul prin adaugarea de noi functionalitati. Datorita acestei flexibilitati si a structurii modulare, G Data il considera a fi deosebit de avansat si de periculos.

Analiza rootkit-ului Uroburos poate fi gasita pe G DATA SecurityBlog:
https://blog.gdatasoftware.com/blog/article/uroburos-rootkit-belgian-foreign-ministry-stricken.html

-###-