Shamoon briše sadržaj diska i MBR

Istraživači kompanije Securealert analizirali su jedan od najgorih malvarea koji se je pojavio u zadnje vrijeme. Virus Shamoon uspostavi kontrolu nad inficiranim računalom, zatim obriše kompletan sadržaj računala (dokumente, slike, video snimke i sl.), ali i MBR (Master Boot Record) onemogućavajući tako ponovno podizanje sustava.

Kako navode iz Securealerta i iz Symanteca, još nije do kraja poznato kako se Shamoon širi, pretpostavlja se da dolazi kao attachment u emailu koji zatim treba pokrenuti kako bi infekcija bila uspješna.

Kada se Shamoon jednom instalira na računalo, preuzima potpunu kontrolu nad računalom koje je povezano s internetom te potom koristi to računalo kao proxy ka vanjskom serveru za komandu i kontrolu. Putem proxya napadač inficira druga računala u internoj mreži. Ovakav proces inficiranja i prikupljanja podakata mogao bi svrstati Shamoon u alat za cyber špijunažu.

Budući da Shamoon obriše kompletan sadržaj diska, također i MBR, ponovno podizanje sustava nije moguće, pa će trebati obaviti kompletan proces oporavka sustava. To uključuje zamjenu MBR-a te povezivanje hard diska sa drugim računalom i sl.

Sama činjenica da nakon što dobije tražne podatke briše sve sa diska, uključujući i MBR, svrstava Shamoon u skupinu zlonamjernijih malvera koji su se pojavili u zadnje vrijeme.

Više o ovoj temi pročitajte slijedeći ovaj link [1].

ned, 2012-08-26 16:58 - Ivan Sokač**Vijesti:** Sigurnost [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1088

Links
[1] http://www.networkworld.com/news/2012/081612-shamoon-261706.html
[2] https://sysportal.carnet.hr/taxonomy/term/13