Trojanac Crisis napada virtualne mašine


Trojanac Crisis, koji je otkriven u lipnju, a koji je prvenstveno bio namjenjen Mac računalima dobio je svoju Windows verziju. Prvenstvena meta ovog trojanca, službeno nazvanog W32.Crisis, su VMware mašine, prenosni USB diskovi te Windows Mobile uređaji.
Crisis traga za VMware virtualnim hard diskom na inficiranom računalu, ukoliko ga pronađe potajno se instalira na njega uz pomoć VMware Playera. Kada korisnik pristupa inficiranom virtualnom disku trojanac špijunira sve njegove aktivnosti.

Za distribuciju ove vrste trojanca koriste se tehnike društvenog inženjeringa koje navode korisnika da pokrene datoteku koja izgleda kao Adobe Flash Installer. Nakon pokretanja trojanac vrši identifikaciju operacijskog sustava na zaraženom računalu te sukladno tome pokreće odgovarajući installer.

Ovu vrstu trojanca prvi su otkrili istraživači Symanteca, a nedavno je došla potvrda i od strane Kaspersky Lab-a. Iz Kaspersky Laba navode kako ova vrsta malvera omogućuje krađu i presretanje podataka sa virtualnih mašina uključujući npr. i podatke potrebne za internetsku kupovinu i sl. Također, napominje se kako su autori ovog trojanca uložili velike napore kako trojanac ne bi bilo otkriven od strane antivirusnih programa.

Malver također može inficirati Windows Mobile uređaj koji je povezan sa zaraženim Windows računalom preko *Remote Application Programming Interfacea*. Trenutno je ovim malverom zaražen neznatan broj računala, ali valja napomenuti da to vjerovatno nije konačan broj, jer je otkriven samo na računalima koja štiti antivirus Kaspersky Lab-a i Symanteca.

Mali broj zaraženih računala ukazuje na to da je malver možda namijenjen više ciljanim napadima nego masovnoj infekciji računala.

Više o ovom trojancu pronađite slijedeći ovaj link [1].

ned, 2012-08-26 16:10 - Ivan Sokač**Vijesti:** Sigurnost [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/1087

Links
[1] http://www.symantec.com/connect/blogs/crisis-windows-sneaks-virtual-machines
[2] https://sysportal.carnet.hr./taxonomy/term/13