Bankarski trojanac Jericho

Tvrtka Palo Alto Networks javlja da je otkrivena inačica trojanca BankPatch, namijenjena krađi zaporki i kolačića, kako bi kriminalcima omogućila provaljivanje na on-line račune žrtava. Virus se počeo širiti sa Izraelskih web siteova koji koriste PHP, no disasembliranjem su otkriveni brojni izrazi na rumunjskom jeziku, pa se pretpostavlja da je virus izrađen u Rumunjskoj.

U kodu je navedeno stotinjak domena koje su izložene napadu, uglavnom se radi o bankama. Očito je da je trojanac napravljen kako bi se koristio za financijske prijevare. Ukradene podatke trojanac isporučuje na brojne siteove koji završavaju na ierihon.com, što je rumun**j**ski izraz za Jerihon, pa je po tome virus dobio ime.

Jericho se ubacuje u logon proces, pa se aktivira nakon svakog restarta. Zatim se zakači za aplikacije koje ne pobuđuju sumnju, poput web preglednika, Outlooka ili Skypea. To mu omogućuje da preko njih koristi funkcije iz DLL biblioteka, a da im pri tom ne pristupa izravno, kako ne bi privlačio pažnju.

Nakon pojavljivanja Jericha 20.4.2012. antivirusni softver različitih proizvođača otkrivao ga je u svega 3,2% slučajeva. Nakon tjedan dana to se povećalo na 39%. Autori virusa koristili su trikove da bi izbjegli detekciju virusa, često mijenjajući kod. Otkrivena su 42 različita uzorka virusa, a čini se da 12 od njih ne otkriva niti jedan antivirusni program.

sri, 2012-06-20 10:11 - Aco Dmitrović**Vijesti:** Sigurnost [1]
Kategorije: Antivirus [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1038

Links
[1] https://sysportal.carnet.hr/taxonomy/term/13
[2] https://sysportal.carnet.hr/taxonomy/term/31