Otkrivena nova vrsta malwarea


Kaspersky Lab otkrio je zanimljivu vrstu malwarea, koji sav posao obavlja u radnoj memoriji i za sobom ne ostavlja nikakvu datoteku na disku napadnutog računala. Malware koristi već poznati propust u Javi (CVE-2011-3544 [1]), na način da izvršava Javascript iz okvira koji je umetnut u web stranicu te svoj kriptirani sadržaj umeće izravno u memoriju procesa javaw.exe.

Otkriveno je da se širi preko teasera na stranicama nekolicine ruskih medijskih kuća koje koriste AdFoxove reklame. Malware se ponaša kao bot koji komunicira sa kontrolnim serverom i krade podatke, na primjer povijest korištenja web preglednika ili tehničke podatke o inficiranom računalu. Nakon odgovora kontrolera, na nekoliko različitih načina nastoji onesposobiti UAC (User Access Control), nakon čega može instalirati trojanca Trojan-Spy.Win32.Lurk.

Budući kao osnovu za napad koristi Javu, teoretski postoji opasnost da zarazi računala sa različitim operacijskim sustavima, iako je analiza koju je objavio Kasperski učinjena na Windows računalu. Dobra strana je što ga je lako ukloniti, jednostavnim resetiranjem računala, ali ostaje opasnost da će korisnik ponovo posjetiti zaražene web stranice i iznova se inficirati. Zato je jedini ispravan način zaštite instalacija Oraclove zakrpe, koja se može skinuti na slijedećem linku [2].

Izvorni članak možete pročitati ovdje. [3]

čet, 2012-03-22 19:43 - Ivan Sokač**Vijesti:** Sigurnost [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/969

Links
[1] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3544
[2] http://www.oracle.com/technetwork/topics/security/javacpuoct2011-443431.html
[3] http://www.kaspersky.com/about/news/virus/2012/Unique_fileless_bot_attacks_visitors_to_news_sites
[4] https://sysportal.carnet.hr/taxonomy/term/13