Otkriven botnet od preko 600.000 inficiranih Macova

Apple ima svoje vjerne sljedbenike koji su se dugo vremena ponosili činjenicom da je OS X siguran operacijski sustav, za razliku od MS Windowsa. No nedavno su istraživači otkrili botnet sastavljen od preko šesto tisuća Macova.
Zaraza se prenosi otvaranjem inficiranih web stranica, koje koriste ranjivost jave označenu kao CVE-2012-0507 [1]. Oracle navodi da je ranjivost [2]lako iskoristiti za napad pokretanjem neprovjerenog appleta unutar zaštićene memorije (*sandboxa*). Apple je reagirao, te se zakrpa [3] nudi na njihovom webu od 3. travnja.

Analiza koda pokazuje da napast manipulira Google pretragama, što se dade iskoristiti za usmjeravanje korisnika na zaražene web stranice. Otvaranjem takve stranice na disk se snima izvršna datoteka koja se zatim aktivira. Napast pošalje prijavu računalu koje sadrži listu provaljenih računala, a zatim generira nazive kontrolnih računala, s kojima se povezuje, provjeravajući njihove RSA ključeve. Nakon provjere instalira dodatan maliciozni program.

Vijest je prva objavila ruska antivirusna tvrtka Dr Web, nazvavši napad BackdoorFlashBack.39, dok je F-Secure je napasti dao naziv Trojan-Downloader:OSX/Flashback.*n*, gdje *n* poprima vrijednosti od A do K, zavisno od inačice virusa. Verzija Flashback.C [4] predstavlja se kao instaler za FlashPlayer, tražeći od korisnika da upiše administratorsku zaporku, nakon čega instalira dodatni kod.

Neki su posumnjali u istinitost ovako velike procjene inficiranih računala, navodeći kako kućni korisnici prilikom svakog spajanja dobijaju drugačiju IP adresu, pa se isto računalo može više puta pribrojiti sumi. No istraživači navode da su broj računala dobili iz jedinstvenog identifikatora kojeg generira sam *exploit* i kojim se prijavljuje kontrolnom računalu. Dr Web navodi da su u veljači 2012. napadači iskorištavali ranjivosti CVE-2011-3544 i CVE-2008-5353, da bi u ožujku počeli koristiti novu ranjivost, CVE-2012-0507. Na njihovoj se stranici [5] s nadnevkom 4.4. navodi brojka od 550.000 inficiranih Macova, najviše u SAD, zatim u Kanadi i Velikoj Britaniji. Nakon što su se u otkrivanje malwarea uključile i druge antivirusne tvrtke, ta je brojka narasla na preko šesto tisuća.

uto, 2012-04-10 11:26 - Aco Dmitrović**Vijesti:** Sigurnost [6]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/979

Links
[1] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0507
[2] http://www.oracle.com/technetwork/topics/security/javacpufeb2012verbose-366319.html
[3] http://support.apple.com/kb/HT5228
[4] http://www.f-secure.com/v-descs/trojan-downloader_osx_flashback_c.shtml
[5] http://news.drweb.com/show/?i=2341&lng=en
[6] https://sysportal.carnet.hr/taxonomy/term/13

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr