Zdrojový kód javascript scanneru Jikto

Vložil/a cm3l1k1 [1], 3 Duben, 2007 - 16:38

- Hacking [2]
- Top Secret [3]

Jikto je JavaScriptový mass scanner bezpečnostních chyb (cross-site scripting, sql injection atd.), který se nevědomky spustí na počítači uživatele když vstoupí na webovou stránku, která jej obsahuje. Lze s ním tedy vytvářet síť botnetů scanujících bezpečnostní nedostatky!

Tento script byl poprvé představen Billy Hoffmanem na konferenci ShmooCon [4] a měl demostrovat první krok toho co dokáže. Zdrojové kódy záměrně neuvolnily, ale během konference chlápek vystupující pod nickem LogicX (http://logicx.net/ [5]) si všiml na jakou stránku Hoffman přistupuje a z ní kód stáhnul.

O několik dní později ho zveřejnil na svých stránkách, ale byl zase hned odebrán na požádání Hoffmana. Nicméně dost lidí si ho stihlo stáhnout a já jsem ho pak z blíže nespecifikovaných zdrojů také sehnal (google :]). Takže nyní je jasné, že lidi kteří tento kód opravdu budou využívat (spíš zneužívat) ho již mají a kdokoliv může tak bez svého vědomí být součástí útoku! A právě proti tomu se chci bránit.

Tento kód měl být proof-of-concept (tedy důkaz že to opravdu jde) a neměl se dostat na veřejnost. A opravdu funguje. Jeho účel/funkce lze řídit souborem, který umístíte na webu a zněj si vyčte "co má dělat".

Bylo to však jen otázkou času, kdy ho někdo získá, nebo kdy někdo udělá podobný. Já ho zvěřejnuji, aby se ostatní mohli podívat na to jak funguje a vymyslet jak ochránit svůj stroj, aby se nestal součástí nějakého útoku (ne jen blokováním všech JavaScriptů... JavaScript je pro bezpečnost zlo, ale na spoustě webů se používá). Je lepší vědět o nebezpečí! (což asi někteří nepochopí)

INFO: Zdrojový kód jsem stáhnul kvůli kritice ostatních. Takže aspon víte o nebezpečí a o tom, že si ho stejně každý během pár minut najde na googlu :o/ (výsledek stažení scriptu = 0)

V prohlížeči Firefox se proti zneužití vašeho prohlížeče lze chránit např. extensionem NoScript [6], který blokuje spuštění JavaScriptů na nedůvěryhodných stránkách.

URL článku: https://security-portal.cz/clanky/zdrojov%C3%BD-k%C3%B3d-javascript-scanneru-jikto

Odkazy:
[1] https://security-portal.cz/users/cm3l1k1
[2] https://security-portal.cz/category/tagy/hacking
[3] https://security-portal.cz/category/tagy/top-secret
[4] http://shmoocon.org/
[5] http://logicx.net/
[6] https://addons.mozilla.org/en-US/firefox/addon/722