Neschopnost českých hostingů aneb Spusť si svého IRC bota kde chceš

Vložil/a RubberDuck [1], 19 Září, 2011 - 18:04

- Unsorted [2]

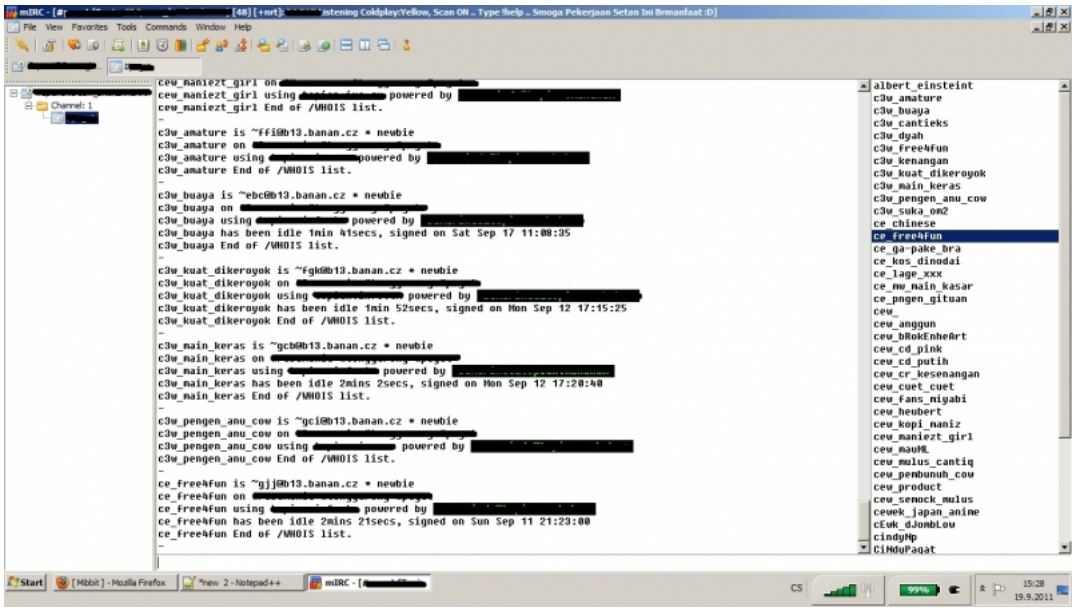
Existenci různých webových botů, crawlerů a spiderů pomalu ale jistě přestává vnímat snad každý administrátor, protože je na jeho serveru/webu častějším hostem než on sám o sobě. Přesto i ostříleného admina dokáže vytočit pohled do logu, kde razí jako pěst na oko pokusy botů exploitovat nejnovější nebo nejrozšířenější zranitelnosti webových aplikací. Po jednom takovém pohledu do logu jsem se rozhodl trochu zapátrat po zdroji těchto pokusů.

Výsledkem mé cesty byl chan na IRC serveru s přibližně padesátkou botů (počet se prakticky neustále měnil v závislosti na aktuálních podmínkách). Sledováním chanu jsem strávil několik dní.

Jeho samotná existence není ničím zvláštním. Snad až na skutečnost, že tento chan hostil z 90% boty ze 2 českých a jednoho slovenského hostingu!! To mě překvapilo. Obzvláště, když administraci a osazenstvo tvořili indové, malajci a podobné národnosti.

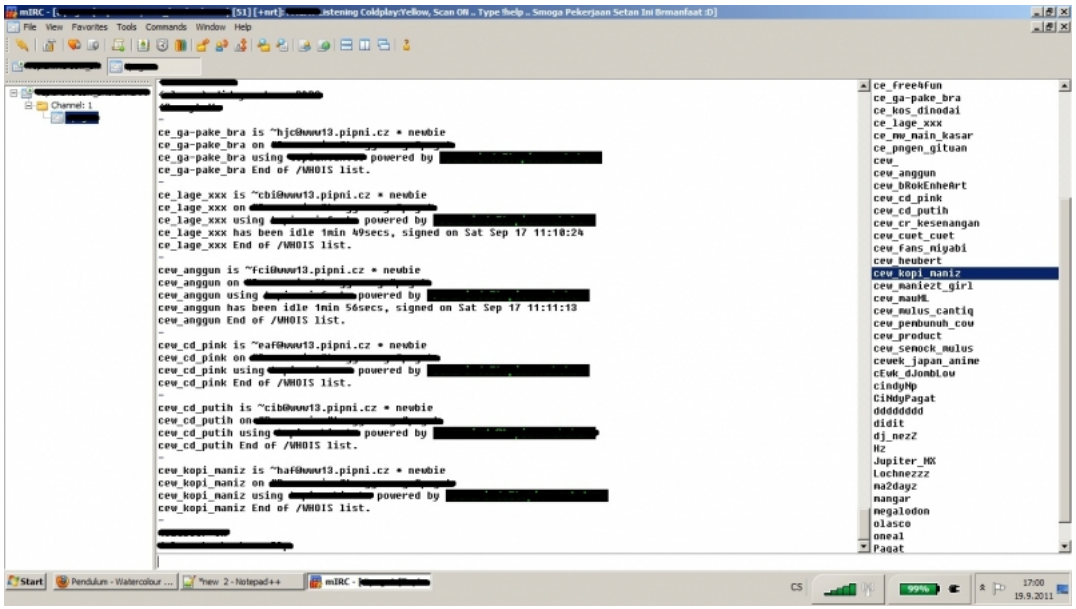
Prakticky hned první den jeden český a jeden slovenský hosting přítomnost botů odhalil a takříkajíc jim "zatnul tipec" (bohužel mě nenapadlo udělat screeny, a proto ani jednu společnost nebudu jmenovat). Tím pádem se počet botů na chanu přiblížil patnáctce kousků. Po sedmi dnech sledování z původních hostů zůstal jen český hosting (je to ten, který se schovává za exotické ovoce a vydává se za nejlepší hosting v ČR - jmenovat ho nebudu, abych mu nedělal reklamu, což by jeho majiteli jistě udělalo velikou radost). Toho však doplnil další český hosting - pípni - a několik málo (asi 3?) dalších zahraničních hostingů.

Nevím, zda je (z pohledu indů) nějaký zvýšený zájem o české hostingy, každopádně je alarmující, že tyto stroje administrují naprosto retardované osoby, které nedokažou zjistit přítomnost botů a tyto odstranit. Provozovatelé takových hostingů by se měli zamyslet nad tím, koho zaměstnávají a v koho vkládají svou důvěru. Provozovateli autodopravy by se asi taky nelíbilo, kdyby si jeho auta jen tak, zadarmo, pujčovali lidé k projížďkám.



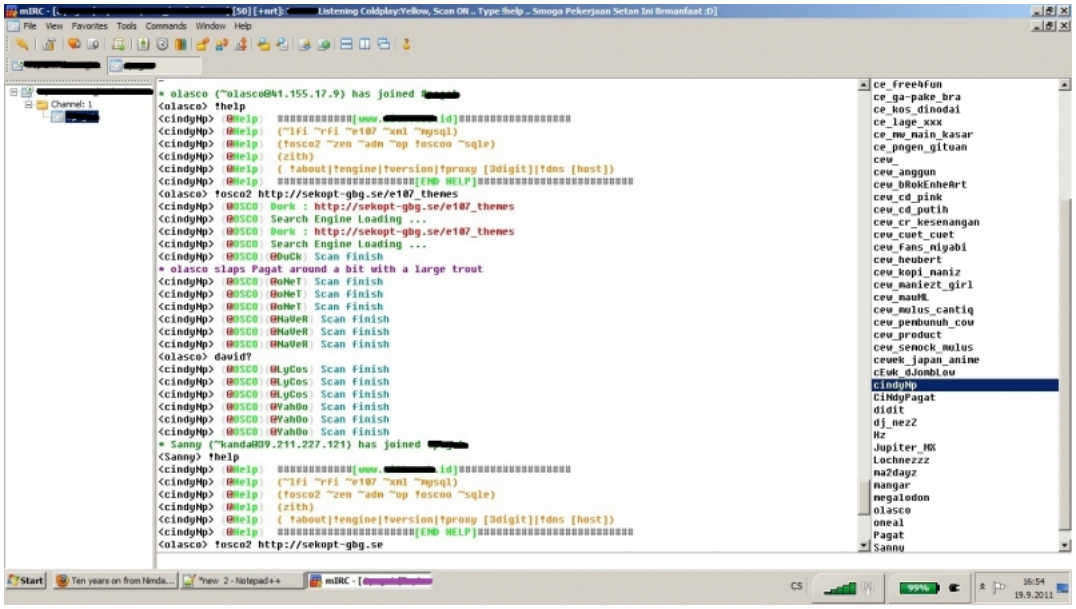
[3]

Sedm dnů na odhalení desítky IRC botů je pro zelináře příliš málo.



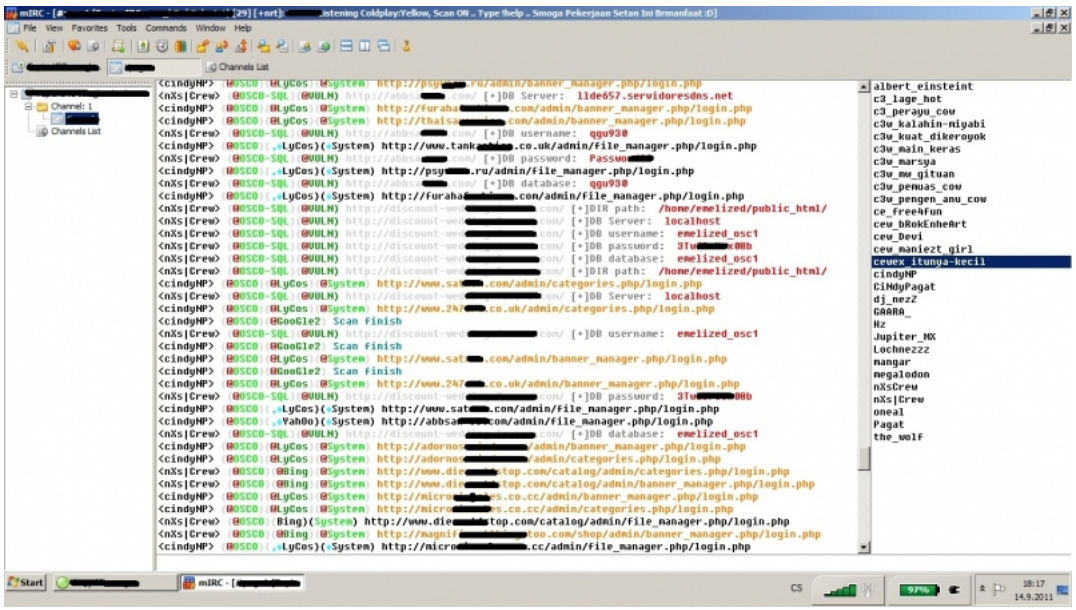
[4]

Snad nepůjde pípni ve stomách zelinářů.



[5]

Boti v akci!



[6]

Boti umí z exploitnutých webových aplikací získat údaje k databázi.

URL článku:
https://security-portal.cz/blog/neschopnost-%C4%8Desk%C3%BDch-hosting%C5%AF-aneb-spus%C5%A5-si-sv%C3%A9ho-irc-bota-kde-chce%C5%A1

Odkazy:
[1] https://security-portal.cz/users/rubberduck
[2] https://security-portal.cz/category/tagy/unsorted
[3] http://security-portal.cz/sites/default/files/IRC_ovoce.jpg
[4] http://security-portal.cz/sites/default/files/IRC_pipni.jpg
[5] http://security-portal.cz/sites/default/files/IRC_search.jpg
[6] http://security-portal.cz/sites/default/files/IRC_mysql.jpg