

Neschopnost českých hostingů aneb Spuť si svého IRC bota kde chceš

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

- [Unsorted](#) [2]

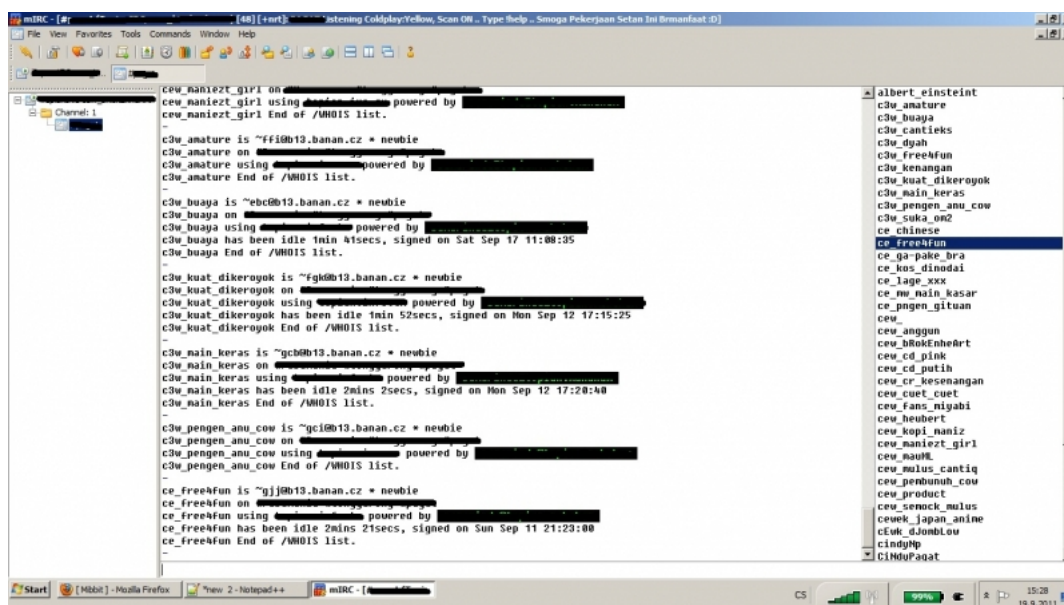
Existenci různých webových botů, crawlerů a spiderů pomalu ale jistě přestává vnímat snad každý administrátor, protože je na jeho serveru/webu častějším hostem než on sám o sobě. Přesto i ostříleného admína dokáže vytočit pohled do logu, kde razí jako pěst na oko pokusy botů exploitovat nejnovější nebo 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 hostingů!! 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 takřkajíc 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 nedokážou zjistit přítomnost botů a tyto odstranit. Provozovatelé takových hostingů by se měli zamyslet nad tím, koho zaměstnávají a v koho vkládají svou důvěru. Provozovatelé autodopravy by se asi taky nelíbilo, kdyby si jeho auta jen tak, zadarmo, půjčovali lidé k projíždkám.



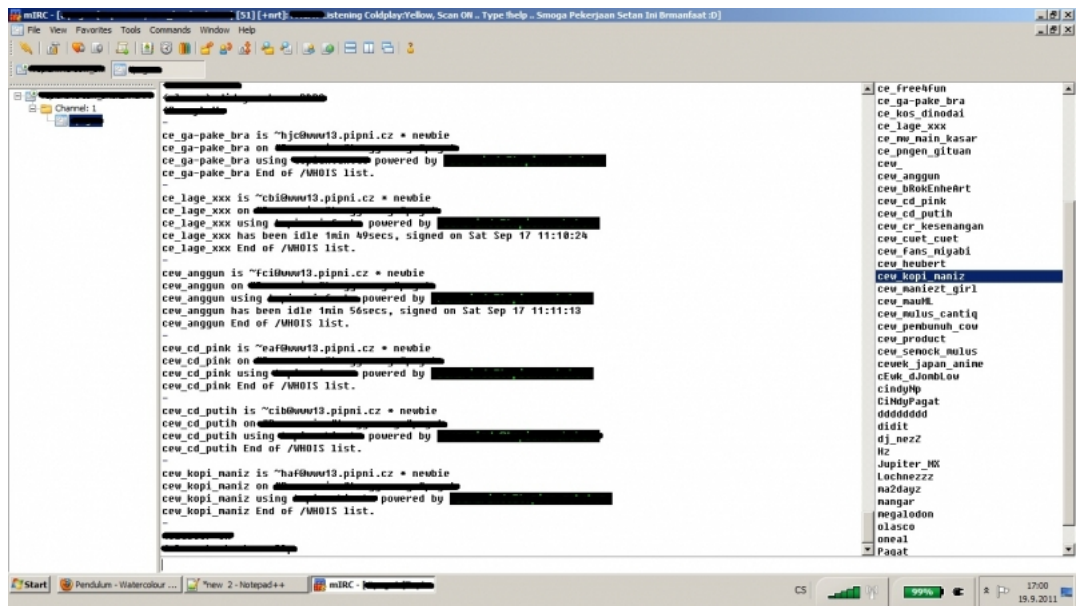
```
mIRC - [#] [48] [+nt] - istening Coldplay\Yellow, Scan OK - Type Help - Smoga Pekerjaan Setlan Inu Bermanfaat (D)
File View Favorites Tools Comments Window Help
Channel: 1
c3w_naniezt_girl on [redacted] powered by [redacted]
c3w_naniezt_girl using [redacted]
c3w_naniezt_girl End of /WHOIS list.
-
c3w_amature is ~ff10@13.banan.cz * neubie
c3w_amature on [redacted]
c3w_amature using [redacted] powered by [redacted]
c3w_amature End of /WHOIS list.
-
c3w_buaya is ~ebc0@13.banan.cz * neubie
c3w_buaya on [redacted]
c3w_buaya using [redacted] powered by [redacted]
c3w_buaya has been idle 1min 41secs, signed on Sat Sep 17 11:08:35
c3w_buaya End of /WHOIS list.
-
c3w_kuat_dikeroyok is ~fg10@13.banan.cz * neubie
c3w_kuat_dikeroyok on [redacted]
c3w_kuat_dikeroyok using [redacted] powered by [redacted]
c3w_kuat_dikeroyok has been idle 1min 52secs, signed on Mon Sep 12 17:15:25
c3w_kuat_dikeroyok End of /WHOIS list.
-
c3w_main_keras is ~gcb0@13.banan.cz * neubie
c3w_main_keras on [redacted]
c3w_main_keras using [redacted] powered by [redacted]
c3w_main_keras has been idle 2mins 2secs, signed on Mon Sep 12 17:20:40
c3w_main_keras End of /WHOIS list.
-
c3w_pengen_anu_cow is ~gcl0@13.banan.cz * neubie
c3w_pengen_anu_cow on [redacted]
c3w_pengen_anu_cow using [redacted] powered by [redacted]
c3w_pengen_anu_cow End of /WHOIS list.
-
ce_free4fun is ~gjj0@13.banan.cz * neubie
ce_free4fun on [redacted]
ce_free4fun using [redacted] powered by [redacted]
ce_free4fun has been idle 2mins 21secs, signed on Sun Sep 11 21:23:00
ce_free4fun End of /WHOIS list.
-
albert_einsteint
c3w_amature
c3w_buaya
c3w_cantieks
c3w_dyah
c3w_free4fun
c3w_kenangan
c3w_kuat_dikeroyok
c3w_main_keras
c3w_pengen_anu_cow
c3w_suka_on2
ce_chinese
ce_free4fun
ce_ga_pake_bra
ce_kos_dinodai
ce_lage_xxx
ce_mv_main_kasar
ce_pngen_gitan
cew
cew_anggun
cew_bRoKEnHeArT
cew_cd_pink
cew_cd_putih
cew_cr_kenangan
cew_cuet_cuet
cew_fans_niyabi
cew_heubert
cew_kopi_maniz
cew_naniezt_girl
cew_nauRl
cew_mulus_cantiq
cew_pembanuh_cow
cew_product
cew_senock_mulus
cewek_japan_anine
c3w_gJombLoo
cingmp
CINMuPaqat
```

[3]

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

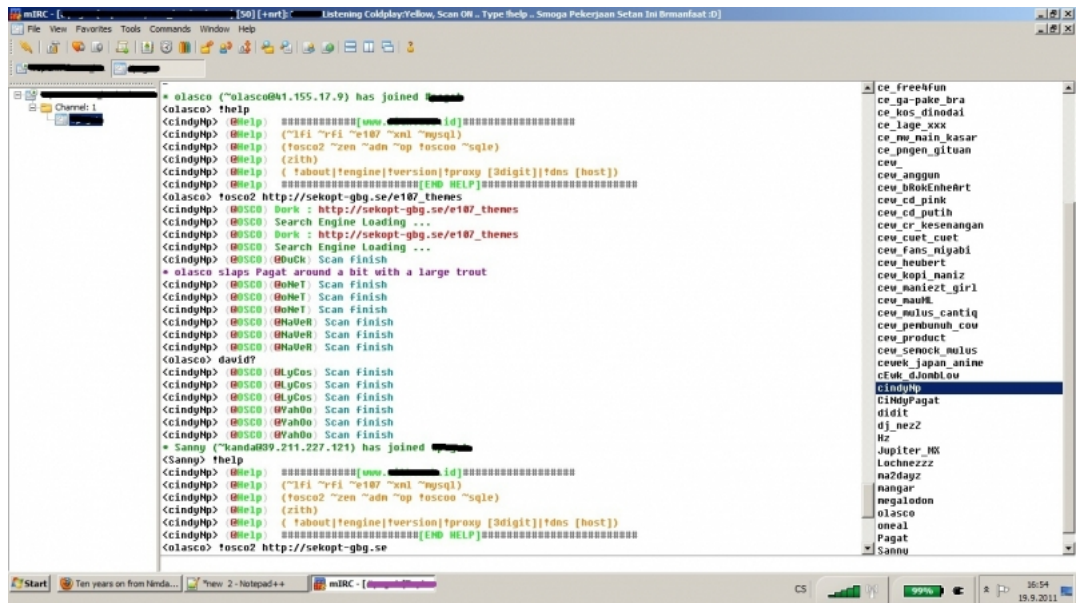
Neschopnost českých hostingů aneb Spust' si svého IRC bota kde chceš

Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)



[4]

Snad nepůjde pípni ve stomách zelinářů.

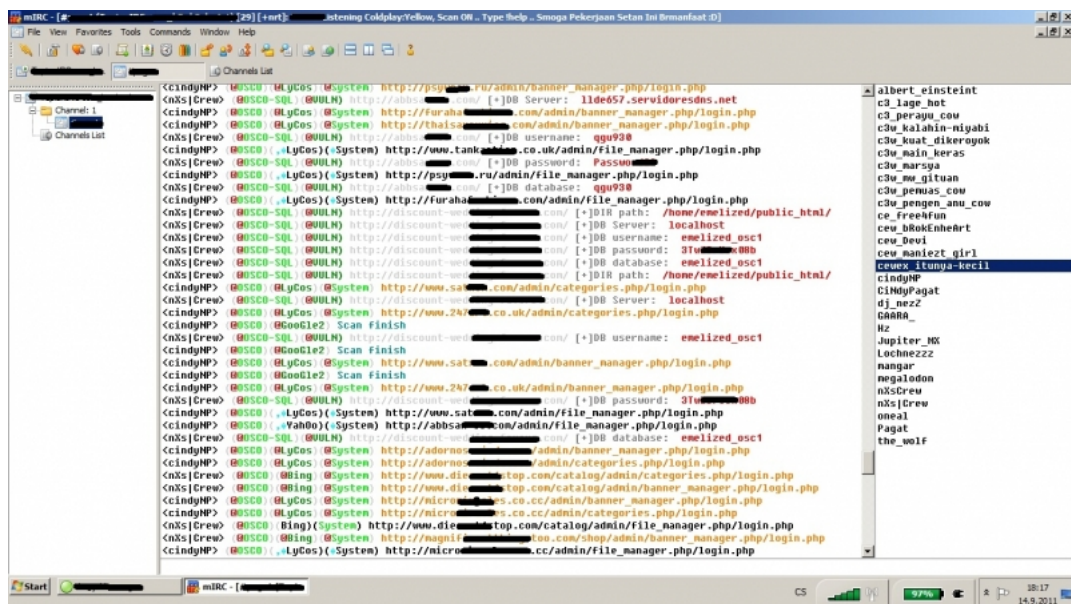


[5]

Boti v akci!

Neschopnost českých hostingů aneb Spusť si svého IRC bota kde chceš

Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)



[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