Síla BOTNETU

Jakub Alimov

jakub.alimov@alinet.cz

Kdo je Jakub Alimov

- Nezávislý badatel v internetové bezpečnosti

  http://cz.linkedin.com/pub/jakub-alimov/20/b10/332
- Mail solutions – bezpečný, bez virů, bez spamů, dostupný digitalní podpis
- Spam… to je můj denní chléb

Obsah

- Co je to botnet
- Ukázka infikace botnetem (je to snadné)
- Síla botnetu
- Prostor pro Vaše otázky

Co je to botnet

- Škodlivý software
  - AdWare
  - MalWare
  - SpyWare
  - SPAM
  - DoS, DDoS
- Infikuje PC => Zombie (botnet +30 000 000)
- C&C servery
- Sofistikované

O co můžete přijít?

- Peníze na Vašich kreditních kartách
- Kontakty, jiné osobní údaje, e-maily
- Výkon Vašeho PC
- Veškerá data ve Vašem PC

Jak se bránit?

- Aktualizovaný OS – dnes již standart
- Antivirový program – účinné!
- Firewall – první signál?
- Výkon PC – velká nápověda

- Spousta ochrany lze řešit již na cestě ke klientskému PC – na straně serveru

PARANOIA: Bezpečné PC je vypnuté PC

Botnet Mapa?

- Botnet mapa podle: Country Code

  http://www.alinet.cz/botnet/geomap.html
- Botnet mapa podle: IP

  http://www.alinet.cz/botnet/mapa.php

  (zakresleno random 1k IP adres)

Ukázka infikace

- Virtualní stroj s Windows XP SP2
- E-mail
- Připojení k internetu
  - Spamování
  - TDL4

Síla botnetu

- White paper

  Denial of Service attacks against DNS servers using the white horses

  http://www.zone-h.org/news/id/4739
- Autor: Boris Mutina, Jakub Alimov

Síla botnetu - teorie

The RFC 2821 (3.6) říká:

”Only resolvable, fully-qualified, domain names (FQDNs) are permitted when domain names are used in SMTP. In other words, names that can be resolved to MX RRs or A RRs (as discussed in section 5) are permitted, as are CNAME RRs whose targets can be resolved, in turn, to MX or A RRs. Local nicknames or unqualified names MUST NOT be used.”

Síla botnetu - příprava

- (Před)registrujem doménu trucsite.com
- Změníme DNS záznam (počkáme)
- Začnem posílat spam jako odesilatel cokoliv@randomHASH.truscite.com
- James@6agux4rs.trucsite.com

Síla botnetu – DNS příprava

```
;; QUESTION SECTION:
;trucsite.com.                  IN      ANY

;; ANSWER SECTION:
trucsite.com.           3592    IN      A       255.255.255.255
trucsite.com.           3592    IN      NS      ns1.trucsite.com.
trucsite.com.           3592    IN      NS      ns2.trucsite.com.
```

```
;; QUESTION SECTION:
;ns1.trucsite.com.              IN      A

;; ANSWER SECTION:
ns1.trucsite.com.       3351    IN      A       95.64.10.70
```

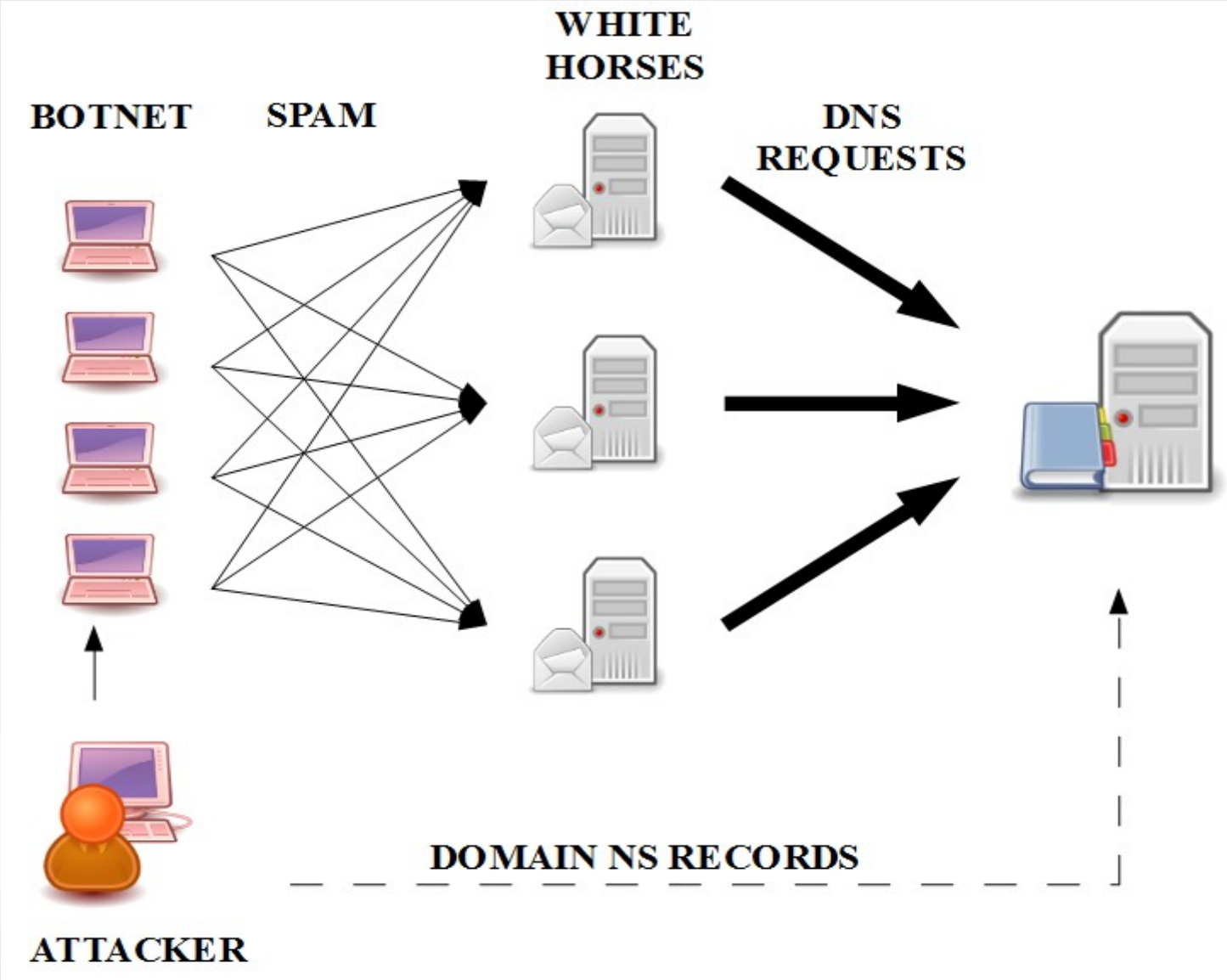
```
;; QUESTION SECTION:
;ns2.trucsite.com.              IN      A

;; ANSWER SECTION:
ns2.trucsite.com.       3522    IN      A       95.64.10.70
```

Síla botnetu - výsledek

- Na IP 95.64.10.70 je DDoS na DNS service

Síla botnetu - výsledek



Síla botnetu - vzorec

- Výsledký útok = (Počet domén$_{[1\sim1000ks]}$ X Počet NS serverů$_{[1\sim1000ks]}$ X Počet spamů$_{[1\sim1x10\^{}6ks]}$ X Počet WH$_{[1\sim1000ks]}$ X Počet query od WH$_{[\sim3ks]}$)

  = nápor na Vaše DNS servery, na Vaši konektivitu

  - DNS down = no mails, no www, no internals,no services, no netowork?

PARANOIA: Bezpečné PC je vypnuté PC

Otázky?

- Děkuji Vám za pozornost

- Jakub.Alimov@alinet.cz