Antispamové technologie

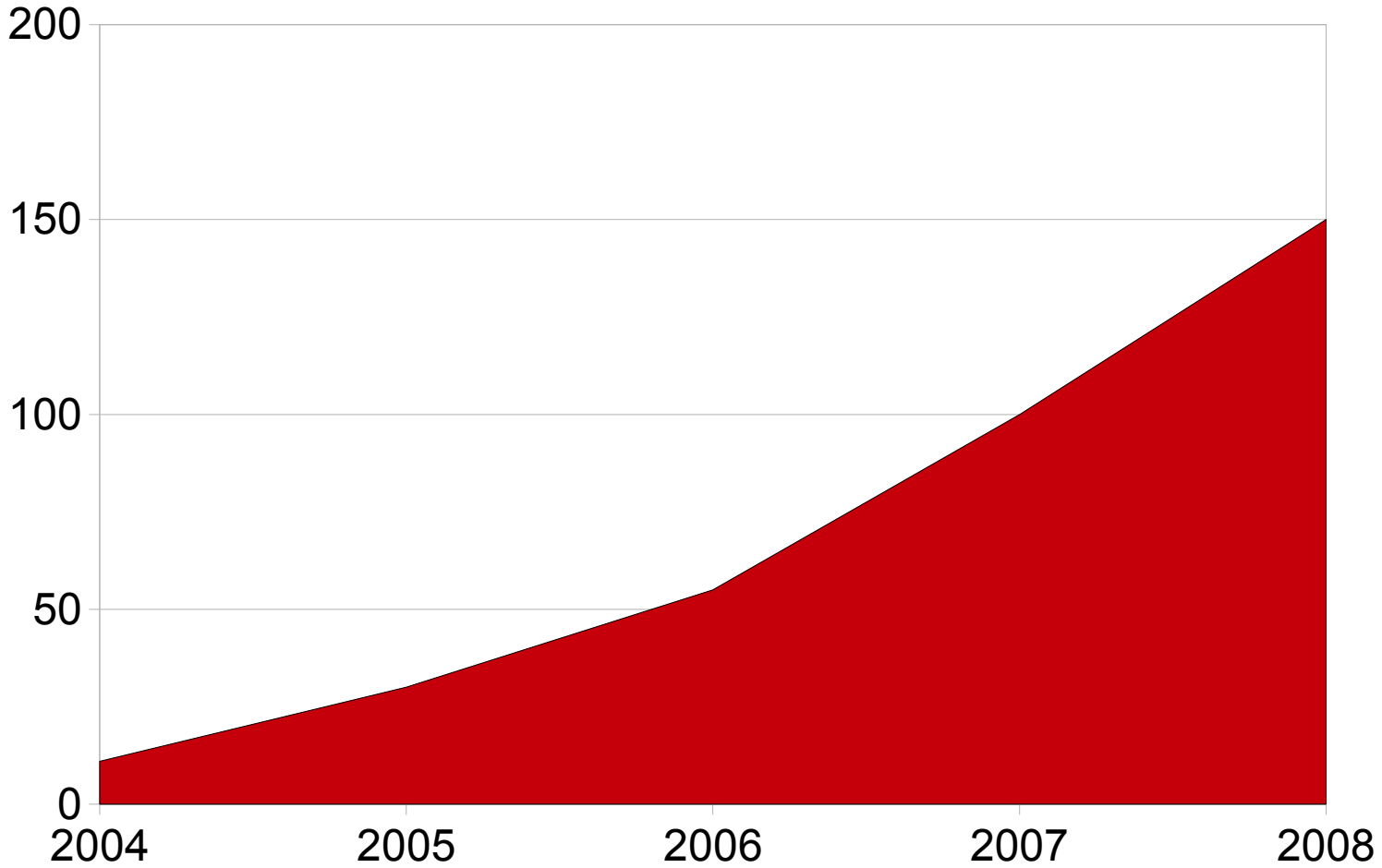
CZ.NIC z.s.p.o.
Petr Hruška
petr.hruska@nic.cz
4. 6. 2009

Statistiky

- první spam odeslán už v roce 1978
- prudký nárůst s rozvojem internetu (2003)
- v roce 2005 překročila míra spamu 80 %
- nyní okolo 80 až 90 %
- velký rozptyl (4x až 9x víc než běžný email)
- absolutní množství spamu roste společně s internetem

Odhadované množství spamu

dnes okolo 200 miliard spamových zpráv denně

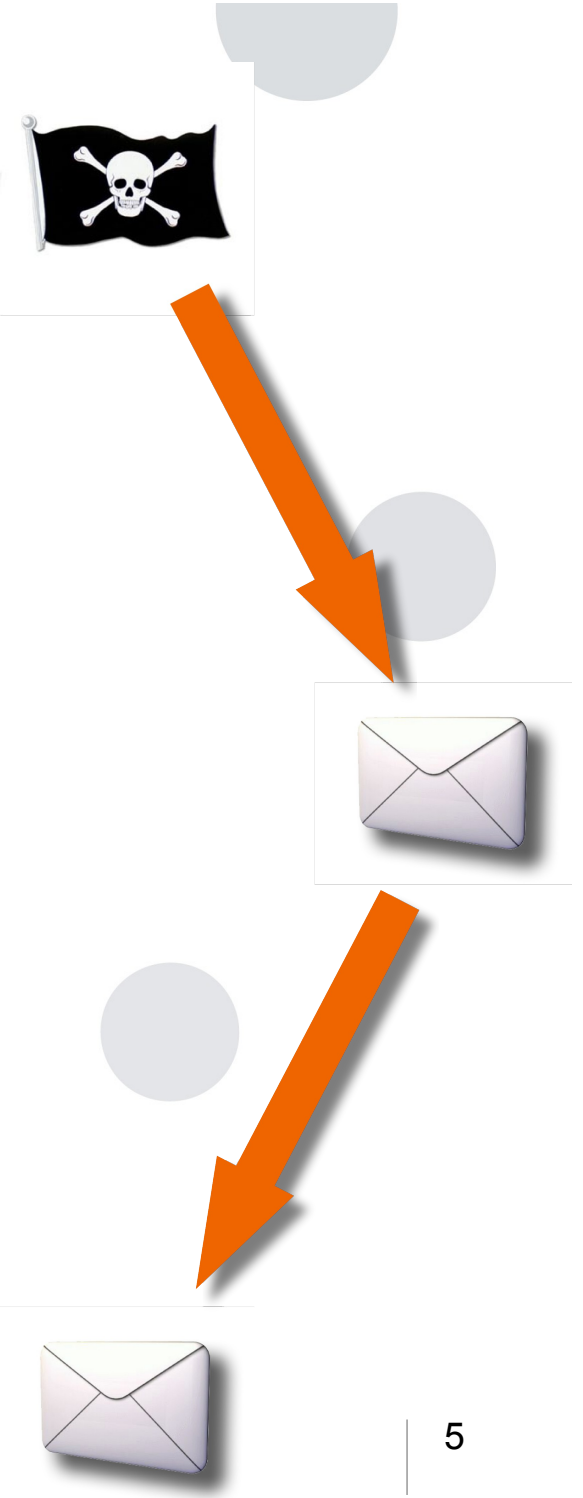


Zdroje spamu

- 95% spamu je odesíláno ze zombie počítačů v botnetech
- podle spamhaus.org pochází 80% spamu od cca 400 lidí
- největší botnety mají miliony zombie
- za 1. čtvrtletí 2009 infikováno přes 10 milionů zombie
- jeden zombie dokáže odeslat až desetitisíce emailů za hodinu

Odpovídání na email

- spamy mají podvrženou adresu odesílatele, která ale ve skutečnosti existuje
- odmítne-li příjemce email a informuje o tom "odesílatele", přepošle mu tak vlastně spam
- na spamy se neodpovídá
- spam zlikvidoval spolehlivost emailu



Anonymita emailu

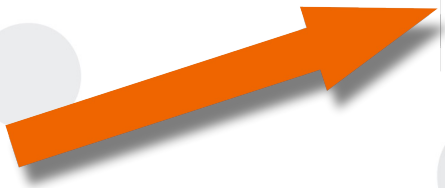
- kdyby nebylo možné podvrhnout adresu odesílatele, měly by odpovědi smysl
- spolehlivost emailu by se zvýšila
- počet zombie počítačů by se snížil, bylo by možné informovat majitele
- část metod se zaměřuje právě na omezení anonymity

Anonymita emailu

CZ.NIC

info@dnssec.cz

čínský hotel



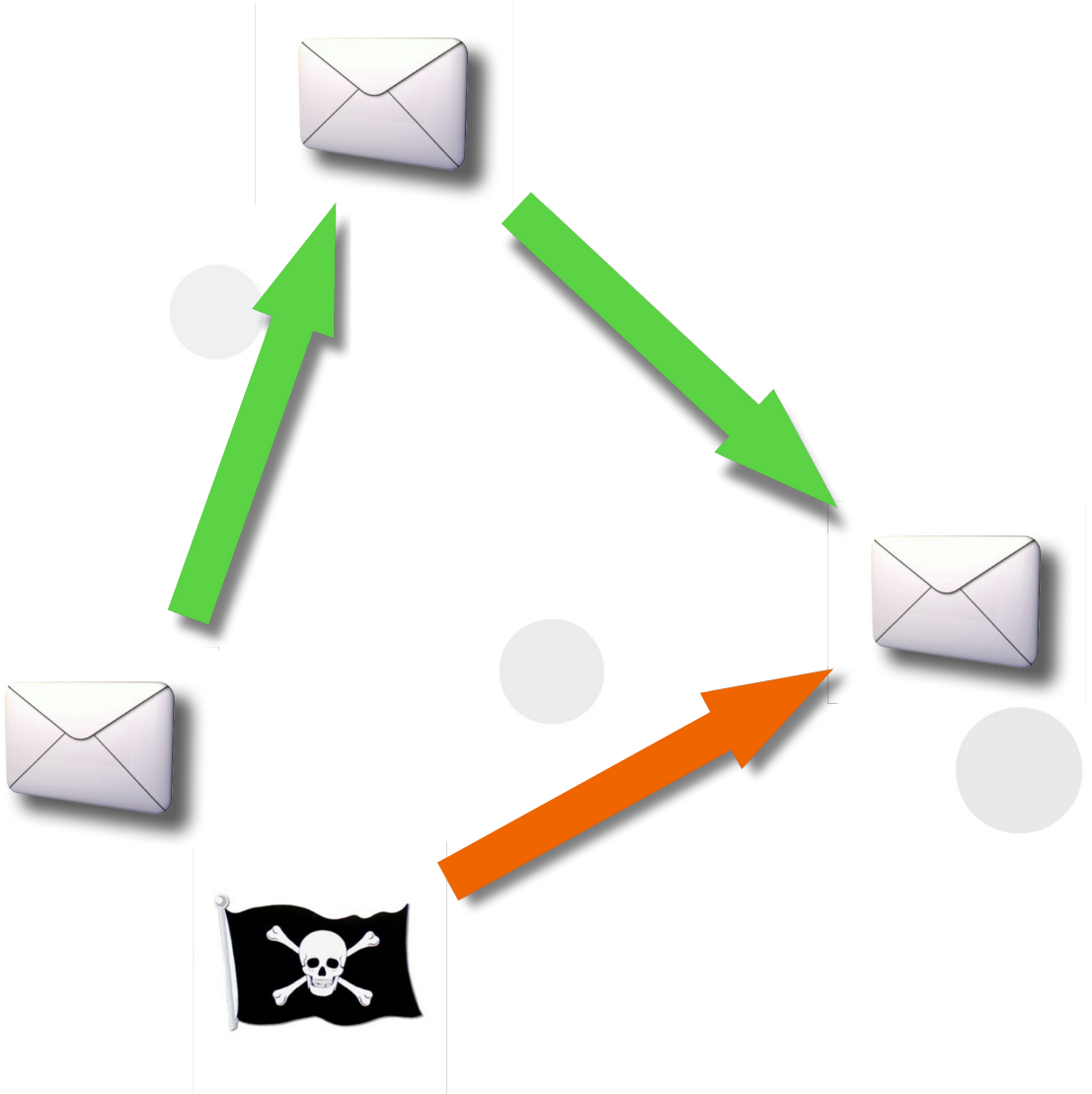
?

SPF (Sender Policy Framework)

- emaily z domény nic.cz je možné posílat odkudkoliv na světě, zcela anonymně
- díky SPF je možné zveřejnit v DNS seznam IP adres používaných pro odesílání emailů z nic.cz
- spammeři by se museli zmocnit serverů nic.cz, aby mohli odesílat emaily vyhovující SPF

MSA (Mail Submission Agent)

CZ.NIC



info@dnssec.cz

SPF (Sender Policy Framework)

- bohužel, uživatelé jsou zvyklí odesílat email odkudkoliv, museli by začít používat MSA
- v ČR má SPF záznamy jen 2 až 3% domén
- v zahraničí 10 až 20%

host -t TXT priklad-spf.cz

v=spf1 mx -all

Blacklisty

- veřejně dostupné seznamy IP adres, ze kterých přichází spam, nebo nějakým jiným způsobem škodí
- příjemce může na základě blacklistu rovnou odmítnout spojení
- tímto způsobem lze odfiltrovat až 75% spamu
- blacklisty se vytvářejí na základě spamtraps, nebo preventivně ve spolupráci s ISP

Filtrování odkazů

- většina spamu obsahuje odkaz na webové stránky
  - často jde o stránky se škodlivým obsahem využívající bezpečnostní nedostatky internetových prohlížečů
- u přijatých emailů je prohledán obsah a je-li nalezen závadný odkaz, je email zahozen
- zbude asi 8% původního spamu

Filtry obsahu

- emaily, které projdou blacklisty, jsou podrobeny strojové analýze obsahu
- hledají se klíčová slova, která se nejčastěji vyskytují ve spamech
- další charakteristické prvky, například specifický tvar hlaviček emailu
- nejznámější open source řešení je SpamAssassin

SpamAssassin

- každému emailu je přiřazeno skóre
- záporné hodnoty znamenají, že email spíše není spam
- kladné hodnoty znamenají, že email může být spam
- emaily se zahazují je-li skóre větší než 5.0

SpamAssassin - úspěšnost

- SpamAssassin chybně označí jako spam méně než 0.1% legitimních emailů
- propustí okolo 1.5% spamu
- projde jen několik spamů denně
- okamžitý účinek
- díky filtrům obsahu je email stále použitelný
- ztrácí se motivace pro nasazení technicky čistších řešení

Závěr

- spam je válka ve formě opatření a protiopatření
- nic nenasvědčuje blízkému konci
- používejte SPF
- braňte své počítače proti virům (zombie se už téměř počítají v procentech)

děkuji z pozornost

dotazy?