Jak se útočí na DNS?

CZ.NIC z.s.p.o.
Ondřej Surý
ondrej.sury@nic.cz
9. června 2011

cz nic
cz domain registry

Proč musí DNS fungovat?

- Základní stavební blok Internetu
- Bez DNS nefunguje skoro nic
  - Více jmen na jedné IP adrese
  - …
- Důležitost informací v DNS
  - Bankovnictví (rhybaření, ...)
  - Falešné zprávy (atomový hřib, …)
  - ...

Útoky na DNS

- Změna informací v DNS
  - Změněné informace v DNS
    - Uživatel se dostane na falešné stránky
  - A. DNS server
    - Zásah celého internetu
  - R. DNS server
    - Zásah velkého počtu zákazníků
    -
- Odepření přístupu (DoS)
  - Nedostupnost informací z DNS
  - Nedostupnost stránek
  - A. DNS server
    - Zásah velkého počtu domén
  - R. DNS server
    - Zásah velkého počtu zákazníků

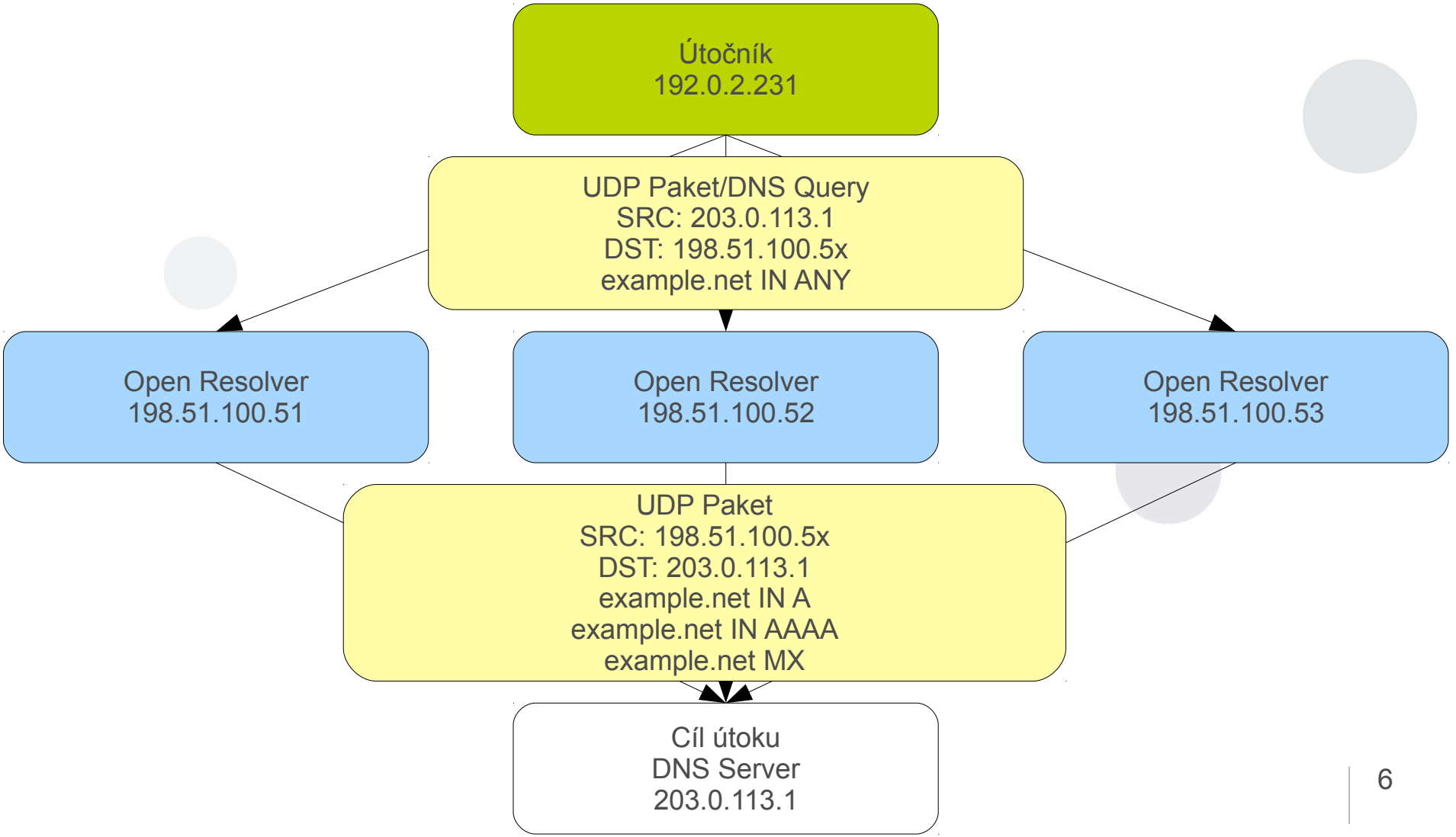
Amplifikační útok (1)

- Varianta DDoS
- Nutné podmínky
  - Ingress Filtering (BCP38)
  - Malý DNS dotaz
  - Velká DNS odpověď
- Co dál pomáhá?
  - Otevřené resolvery
  - Vlastní botnet

Amplifikační útok (2)

- DNS dotazy útočníka
  - Zdrojová IP adresa (cíl útoku)
  - Cílová IP adresa (DNS server)
  - Malý DNS dotaz (~80 bajtů)
    - Hlavička
    - Sekce QUERY (IN ANY)
  - Čím větší DNS odpověď, tím lépe
    - Hlavička
    - ANSWER + AUTHORITY + ADDITIONAL
    - Zvětšení 10-20x !!!

Amplifikační útok (3)



Amplifikační útok – ochrana

- Dostatečná kapacita DNS serverů
  - Dostatečná kapacita linky!
    - Příklad: ICANN L-ROOT
      - 10 Gbps NIX
      - 50 kbps průměrný provoz za poslední měsíc
- Anycast
  - Provoz se rozloží
  - Nebo zasáhne jen část serverů

Útok na DNS operátora

- Různé způsoby
  - Útok na infrastrukturu
    - Registrátora
    - DNS operátora
  - Zjištění hesla odpovědné osoby
    - Sociální inženýring
    - Chyby v software
      - Flash v Excelu
    - Backdoory

From: Наташа Подлый

To: Joe Gullible

Subject: I love you

Hi, I saw you on the internet and I liked you, open the attachment to see my pictures.

Love, Natasha

Attachment: naked.exe

Útok na DNS operátora

- Cílem je získat přístup do administrace DNS
  - Napadení počítače zaměstnance registrátora
  - Napadení počítače zaměstnance cíle útoku
- Twitter.com
  - Změna v DNS u registrátora autorizována platnými přístupovými údaji
- Baidu.com
  - Změna DNS u registrátora

Útok na DNS operátora – ochrana

- Vzdělávání zaměstnanců :)
- Technické možnosti ochrany
  - Zamykání na úrovni registru
  - Více faktorová autentizace
  - …

Útok na cache rekurzivního DNS

- „Velká“ prezentace na IT10
  - http://www.nic.cz/it10/
- Podmínky útoku
  - Rychlý internet
  - BCP38 (možnost falšovat zdrojovou adresu)
- Lepší podmínky útoku
  - DNS „zabezpečeno“ pouze ID v hlavičce DNS
  - Nedostatečně náhodný zdrojový port

Útok na cache rekurzivního DNS

- Kaminsky-style útok
  - Vlastnost protokolu
  - Dotaz na <xyz-rnd>.example.net
    - Odpověď není/nemůže být v cache
    - Podvržené údaje jsou v AUTHORITY sekci
- Současnost
  - Statické porty – napadnutelnost v řádu sekund
    - Nízké nároky na hardware i propustnost sítě
  - Náhodné port – napadnutelnost v řádu dní
    - Vyšší nároky na hardware i propustnost sítě

Studie náhodnosti portů pro .CZ

- Analýza DNS provozu na autoritativních DNS
  - Projekt DITL 2011
    - http://www.caida.org/projects/ditl/
    - 24 hodin provozu
  - Analýza DNS resolverů
    - Statický zdrojový port
    - Sekvenční zdrojové porty
    - Vyřazeny resolvery s méně než tři porty

Studie náhodnosti portů pro .CZ

- Celkový počet resolverů:

  1.660.984
- Z toho resolverů se statickými porty:

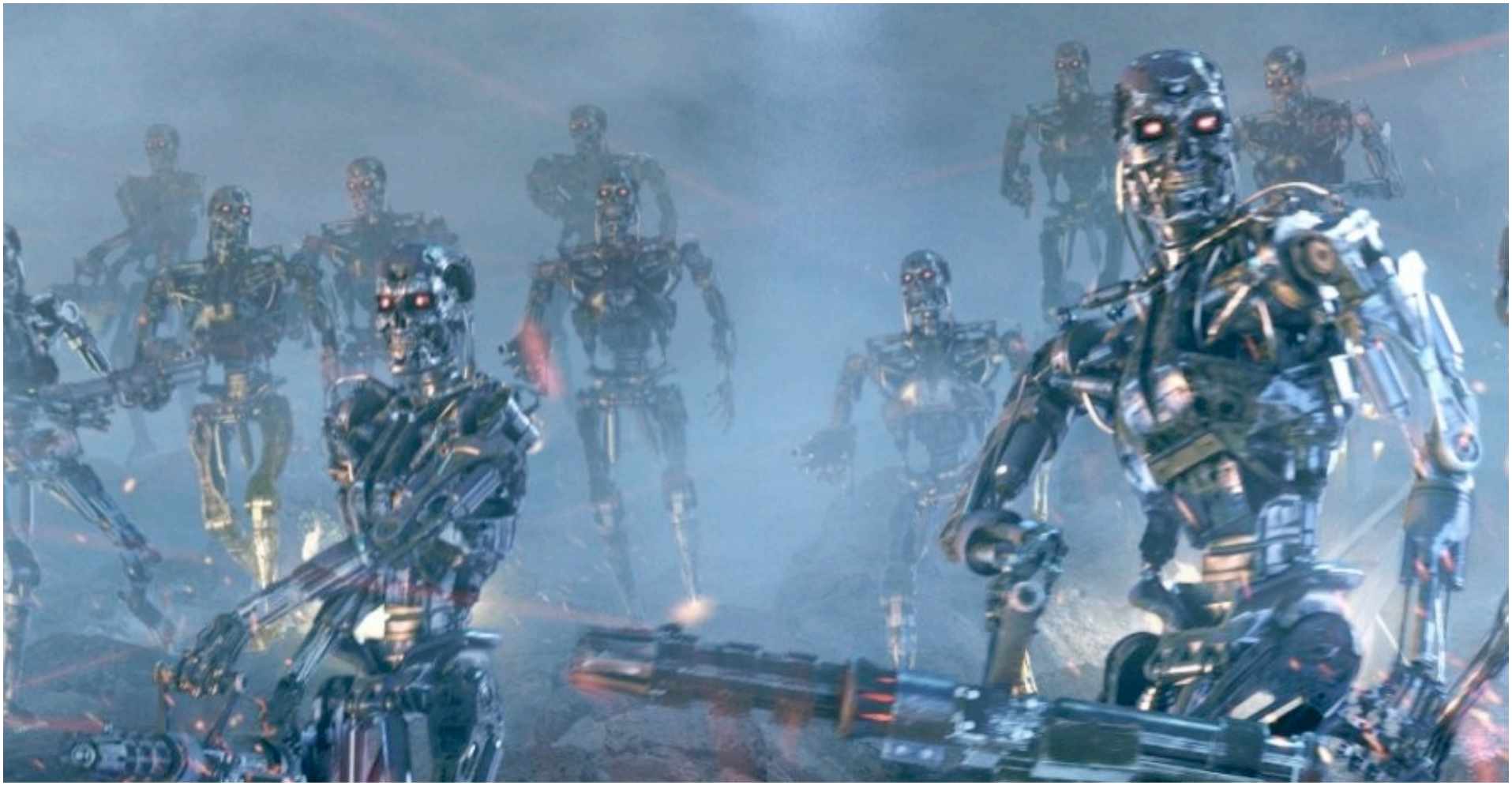
  147.177 (9%)
- Z toho resolverů se sekvenčními porty:

  16.104 (1%)

Statické a sekvenční porty

- Statické porty
  - Napadnutelné v řádu sekund
  - Neaktualizované DNS servery
  - Vážné bezpečnostní riziko!
- Sekvenční porty
  - 88 88 88 333 333 333 … … …
  - S trochou snahy také napadnutelné v řádu sekund
  - I aktualizované DNS servery
    - Za NATem...

Jste v bezpečí?



Jste v bezpečí?

- Pomůže:
  - Omezení dotazů na vlastní síť?
    - Ne, pokud nefiltrujete IP adresy na hraničních směrovačích (BCP38)
  - Znáhodnění zdrojových portů/více DNS serverů?
    - Ne, pouze sníží účinnost útoku
  - Rychlá linka?
    - Ne, pouze sníží účinnost útoku
    - Pořád lze zahltit zdrojový server (amplifikační útok...)

Jste v bezpečí?

- Ingress/Egress filtering všude...
  - Pomohlo by i proti ostatním druhům útoků
  - Ale … „Kdo z vás to má?“
- DNSSEC
  - Informace v DNS jsou podepsané
  - 15% .CZ podepsáno :)
  - Domény v Netmonitoru :(
    - TOP100: 18 domén (18%)
    - TOP200: 37 domén (18%)
    - Vše (481): 77 domén (16%)

Mikrostudie DNSSEC Validátory

- DITL 2011 Data
  - Metodika Guðmundsson & Crocker
    - http://conferences.npl.co.uk/satin/papers/satin2011-Gudmundsson.pdf
- DNSSEC Validátory
  - Největší jsou v zahraničí (Ukrajina...?...?)
  - V Čechách operátoři experimentují

Mikrostudie DNSSEC Validátory

Queries	IP	#DNSKEY	Hostname	Netname
3260094	194.228.41.65	49	dnsnest1.o2isp.cz.	INFOVISTA-NET
3140427	194.228.41.113	52	dnsnest2.o2isp.cz.	INFOVISTA-NET
3097537	160.218.161.54	36	dnsnest3.o2isp.cz.	EUROTEL
2455325	195.34.133.21	13	viedns09.chello.at.	PUBLIC-SERVER-NETWORK
2335356	213.46.172.36	65	cz-prg01a-dns01.chello.cz.	LINKS-CZECH
2271590	93.153.117.5	54	beluga-4.t-mobile.cz.	T-MOBILECZ-GPRS_3G
2254032	93.153.117.3	21	beluga-2.t-mobile.cz.	T-MOBILECZ-GPRS_3G
2226927	93.153.117.2	15	beluga-1.t-mobile.cz.	T-MOBILECZ-GPRS_3G
1525287	193.179.159.138	146	rs1-b.isp.cz.net.	CZ-GTS-950808
1510294	193.179.159.131	153	rs1-e.isp.cz.net.	CZ-GTS-950808
1506195	193.179.159.146	140	rs1-c.isp.cz.net.	CZ-GTS-950808
1505658	193.179.159.130	155	rs1-a.isp.cz.net.	CZ-GTS-950808
1504353	193.179.159.154	158	rs1-d.isp.cz.net.	CZ-GTS-950808
1485300	193.179.159.147	139	rs1-f.isp.cz.net.	CZ-GTS-950808
1433321	212.24.128.8	61	ns.inway.cz.	INWAY
1053551	2a01:5e0::2	100	rns1.sloane.cz.	CZ-SLOANE-20071109
1026111	212.24.132.132	77	ns.inway.net.	INWAY
994002	212.158.128.2	180	cachens.bluetone.cz.	BLUETONE
975424	2a01:5e0::102	93	rns2.sloane.cz.	CZ-SLOANE-20071109
871254	213.46.172.37	53	cz-prg01a-dns02.chello.cz.	LINKS-CZECH

Otázky?