Zranitelnosti v BGP protokolu

CZ.NIC z.s.p.o.
Ondřej Surý
ondrej.sury@nic.cz
4. 6. 2009

Obsah

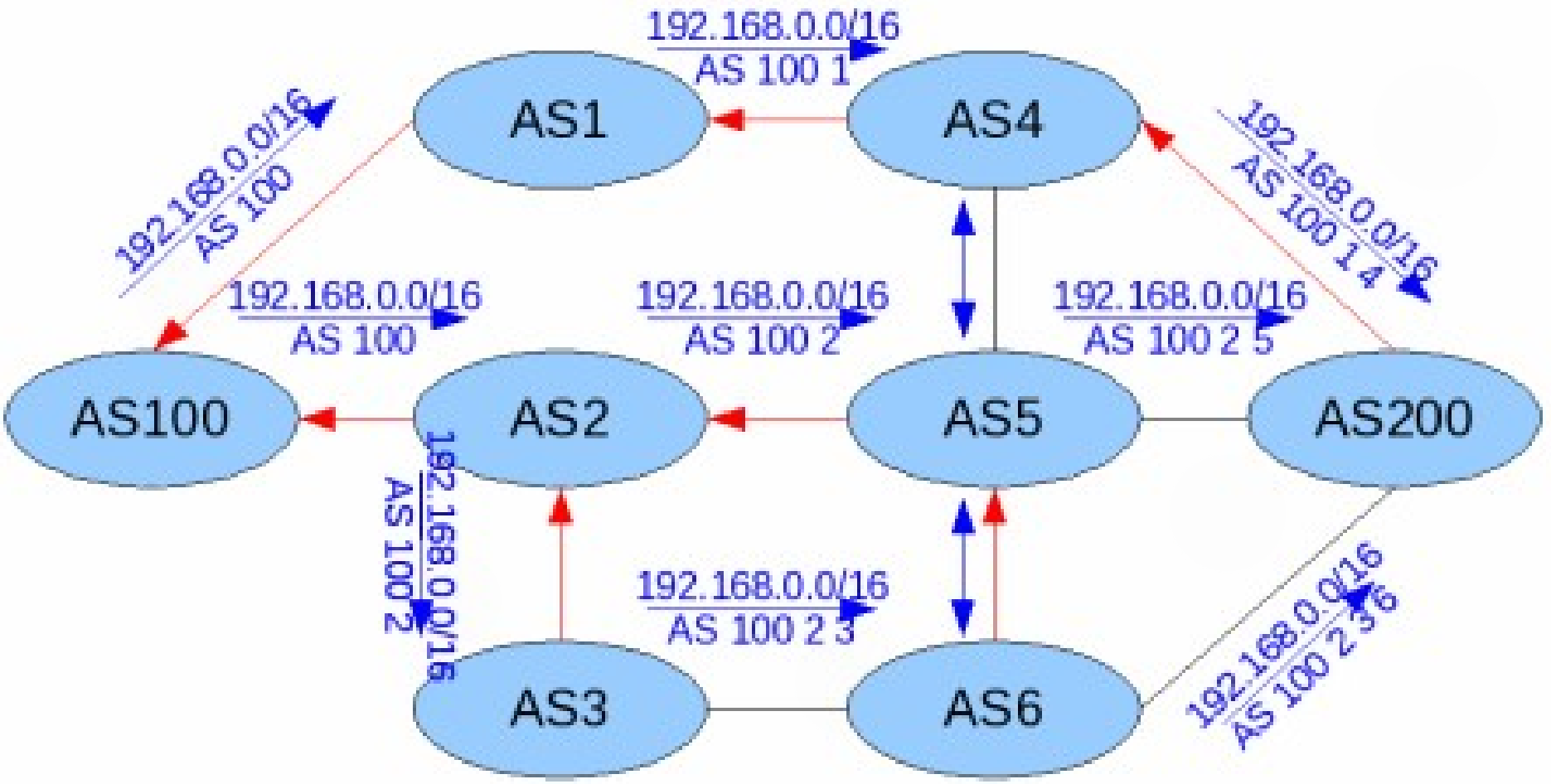
- Co je to Internet?
- Únosy IP adres
- „Neviditelný“ MITM BGP útok (Pilosov&Kapela)
- Možná „řešení“...?

Co je to Internet?

Co je to Internet?

- Žádný centrální mozek lidstva
- Množství nezávislých navzájem propojených sítí (autonomních systémů) pomocí BGP
  - Identifikovaných pomocí čísla AS (ASN)
  - Propagujících rozsahy IP adres
- Propagace obsahuje
  - IP prefix(y)
  - AS_PATH (**Detekce smyček**)
  - Další atributy

Co je to Internet?



Nutné základy BGP

- Kratší AS_PATH vyhrává
  - **192.168.0.0/16 AS 100 1**

    vs.
  - 192.168.0.0/16 AS 100 2 3 6
- Více specifická specifická cesta je lepší
  - **192.168.0.0/17**

    vs.
  - 192.168.0.0/16

Vztahy v BGP

- Peering
  - (Většinou) zdarma
  - 1:1
  - IP rozsahy nejsou distribuovány dále
- Zákazník
  - (Většinou) komerční vztah vůči transitnímu oper.
  - Propagace od zákazníka je posílána dále

Kdo může propagovat...

- Kdokoli...

Kdo může propagovat...

- BGP je založeno na důvěře
  - Žádný centrální mozek lidstva
- ICANN přiděluje IP rozsahy RIRům (RIPE, ARIN, LACNIC, APNIC, AfriNIC)
- RIR přiděluje LIRů (ISP, hostingy, IX, …)
- Neexistuje „silná“ vazba mezi ASN a IP blokem

Předpoklady v BGP

- Každý AS propaguje jen IP rozsahy, které spravuje
- Zdroj aktualizace v BGP je autoritativní pro každou poslanou změnu
- Propagovaná AS_PATH je korektní
- TCP spojení je bezpečné :)

Filtrování

- Zákazníků
  - Často žádné (max-prefix, občas AS_PATH)
  - Menší ISP – statické seznamy
  - Větší ISP – automatizované filtry z IRR
- Peeringy
  - Většinou pouze max-prefix
  - Často nejsou filtrovány ani vlastní prefixy od ostatních peerů

Únos IP adres

- Tradiční
  - Rychlejší než dostat IP blok oficiální cestou :)
  - Spam, scam, boti
  - DoS konkurence, vydírání
  - Podvržení cíle (Twitter, Youtube)

Jak na to?

- Starý freemail/doména ve whois
  - Zaregistrujete email/doménu
  - Změníte kontaktní údaje
  - IP adresy jsou vaše
- Prostě prefix pošlete do světa...
  - Nikdo si toho možná ani nevšimne
  - Nebo jej oficiálně oznamte a pak pošlete
    - Nikdo to nebude kontrolovat...

Únosy IP adres v minulosti

- 134.33.0.0/16 – CODEX (Motorola) – spam
- 146.20.0.0/16 – Erie Forge & Steel – spam
- 166.188.0.0/16 – Carabineros De Chile (2x)
  - „Carabineros De Chile LLC, Nevada Corporation“
- 203.26.80.0/24 – Motorola AU
  - Ilegální pornografie
- 208.65.153.0/24 – Youtube
  - Pakistan Telecom

Zabezpečení proti únosu...

- Musí filtrovat všichni
- BCP – Alert systémy (MyASN, PHAS, Renesys)
- Používejte IRR (alespoň pro sebe)
- Únos není anonymní – díky AS_PATH
- V případě zjištění únosu kontaktujte vaše tranzitní operátory
- Řešení v řádu minut, hodin, dní...

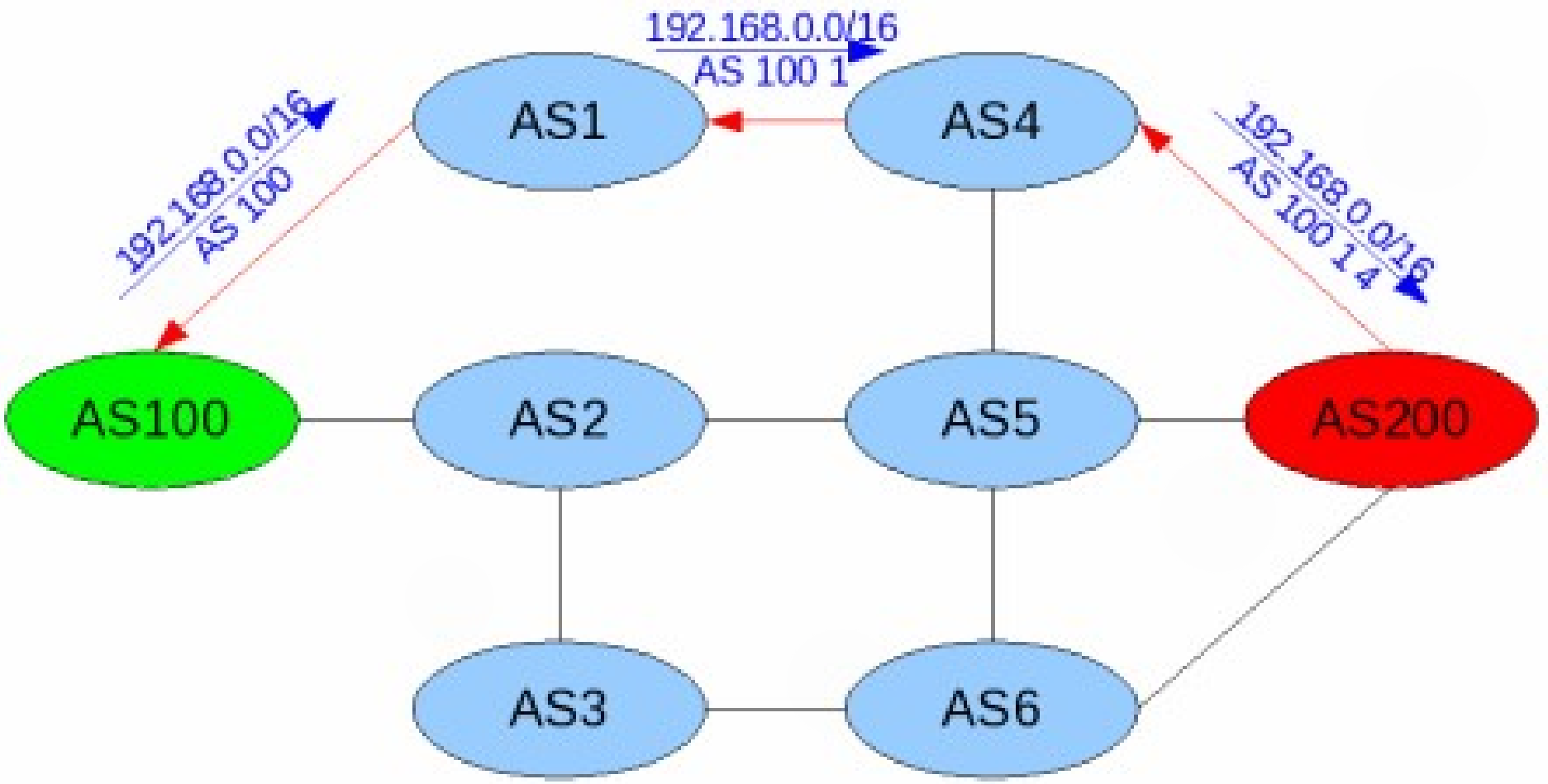
„Neviditelný“ BGP únos

- Pilosov & Kapela
- DEFCON 2008

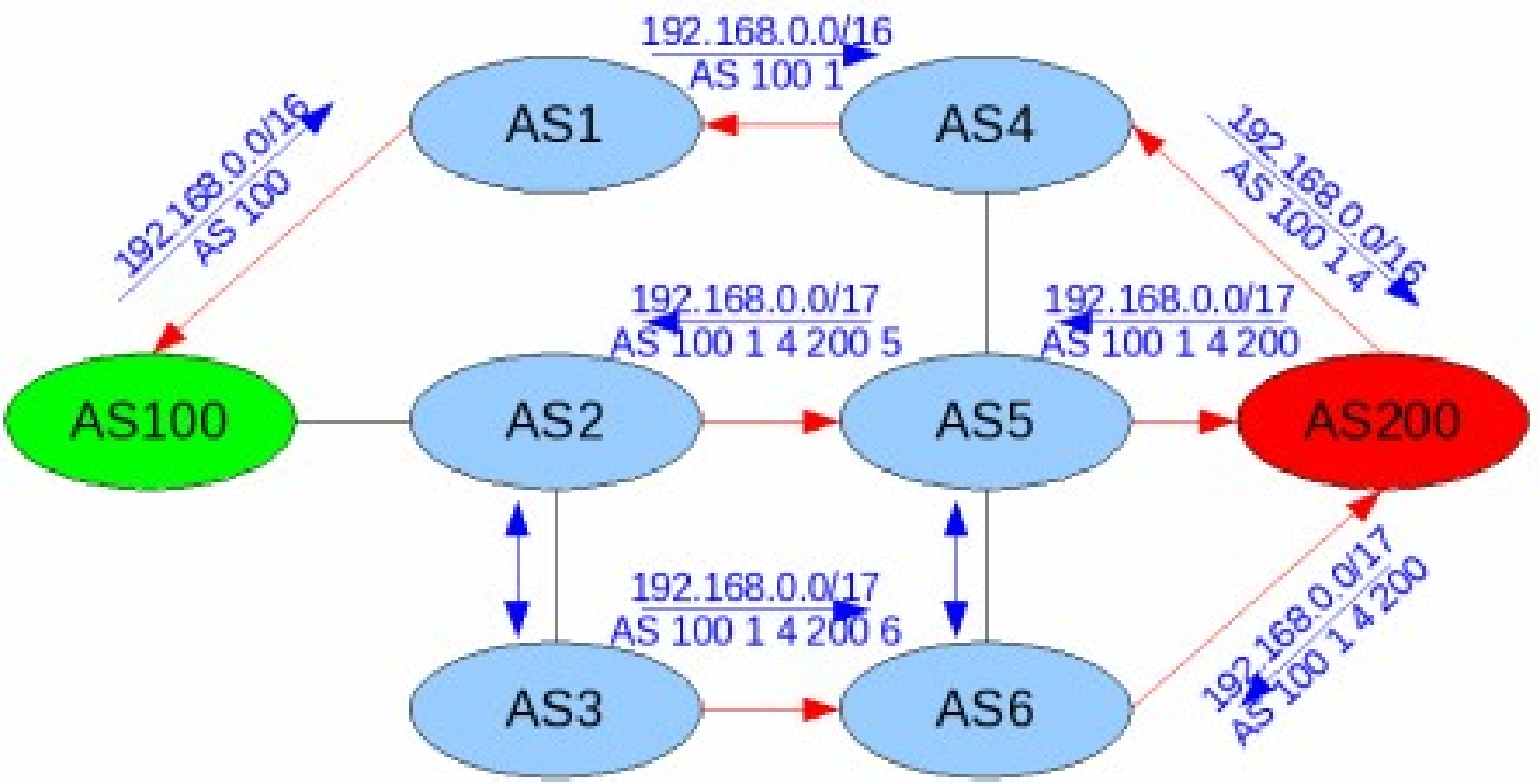
„Neviditelný“ BGP únos

- Uneseme IP prefix jako obvykle
  - Délka prefixu, kratší AS_PATH, atp.
  - Tj. směrovače si budou vybírat vaši „lepší“ cestu
- Nějak musíme provoz zase vrátit zpátky
  - VPN/Tunnel?
  - Potrubní pošta?
- Ne, použijeme Internet a mechanismy BGP

Zjistíme nejkratší cestu zpět



Pošleme „lepší“ prefix



AS_PATH je náš přítel

- Mechanismus detekce smyček v AS_PATH
  - Cesta s vlastním AS už u mě „byla“, tj. nechci ji
- Sítě v nejkratší cestě novou propagaci zahodí
- Všude jinde je náš „lepší“ prefix
- Data přijmeme, zpracujeme a pošleme zpátky
  - Nejkratší cestou, která nezná náš „lepší“ prefix

Ukrytí útočníka

- Delší cesta jde poznat z traceroute (k cíli)
  - Od cíle je provoz stále stejný
- Změníme TTL v IP paketu
  - Pro naše zařízení (plus)
  - Pro odchozí síť (plus)
- Tím skryjeme podezřelou aktivitu

Bez úprav TTL

```
 2 12.87.94.9 [AS 7018] 4 msec 4 msec 8 msec
 3 tbr1.cgcil.ip.att.net (12.122.99.38) [AS 7018] 4 msec 8 msec 4 msec
 4 ggr2.cgcil.ip.att.net (12.123.6.29) [AS 7018] 8 msec 4 msec 8 msec
 5 192.205.35.42 [AS 7018] 4 msec 8 msec 4 msec
 6 cr2-loopback.chd.savvis.net (208.172.2.71) [AS 3561] 24 msec 16 msec 28 msec
 7 cr2-pos-0-0-5-0.NewYork.savvis.net (204.70.192.110) [AS 3561] 28 msec 28 msec 28 msec
 8 204.70.196.70 [AS 3561] 28 msec 32 msec 32 msec
 9 208.175.194.10 [AS 3561] 28 msec 32 msec 32 msec
10 colo-69-31-40-107.pilosoft.com (69.31.40.107) [AS 26627] 32 msec 28 msec 28 msec
11 tge2-3-103.ar1.nyc3.us.nlayer.net (69.31.95.97) [AS 4436] 32 msec 32 msec 32 msec
12 * * *   (missing from trace, 198.32.160.134 – exchange point)
13 tge1-2.fr4.ord.llnw.net (69.28.171.193) [AS 22822] 32 msec 32 msec 40 msec
14 ve6.fr3.ord.llnw.net (69.28.172.41) [AS 22822] 36 msec 32 msec 40 msec
15 tge1-3.fr4.sjc.llnw.net (69.28.171.66) [AS 22822] 84 msec 84 msec 84 msec
16 ve5.fr3.sjc.llnw.net (69.28.171.209) [AS 22822] 96 msec 96 msec 80 msec
17 tge1-1.fr4.lax.llnw.net (69.28.171.117) [AS 22822] 88 msec 92 msec 92 msec
18 tge2-4.fr3.las.llnw.net (69.28.172.85) [AS 22822] 96 msec 96 msec 100 msec
19 switch.ge3-1.fr3.las.llnw.net (208.111.176.2) [AS 22822] 84 msec 88 msec 88 msec
20 gig5-1.esw03.las.switchcommgroup.com (66.209.64.186) [AS 23005] 84 msec 88 msec 88 msec
21 66.209.64.85 [AS 23005] 88 msec 88 msec 88 msec
22 gig0-2.esw07.las.switchcommgroup.com (66.209.64.178) [AS 23005] 88 msec 88 msec 88 msec
23 acs-wireless.demarc.switchcommgroup.com (66.209.64.70) [AS 23005] 88 msec 84 msec 84 msec
```

S úpravami TTL

```
 2 12.87.94.9 [AS 7018] 8 msec 8 msec 4 msec
 3 tbr1.cgcil.ip.att.net (12.122.99.38) [AS 7018] 4 msec 8 msec 8 msec
 4 ggr2.cgcil.ip.att.net (12.123.6.29) [AS 7018] 4 msec 8 msec 4 msec
 5 192.205.35.42 [AS 7018] 8 msec 4 msec 8 msec
 6 cr2-loopback.chd.savvis.net (208.172.2.71) [AS 3561] 16 msec 12 msec *
 7 cr2-pos-0-0-5-0.NewYork.savvis.net (204.70.192.110) [AS 3561] 28 msec 32 msec 32 msec
 8 204.70.196.70 [AS 3561] 28 msec 32 msec 32 msec
 9 208.175.194.10 [AS 3561] 32 msec 32 msec 32 msec
10 gig5-1.esw03.las.switchcommgroup.com (66.209.64.186) [AS 23005] 88 msec 88 msec 84 msec
11 66.209.64.85 [AS 23005] 88 msec 88 msec 88 msec
12 gig0-2.esw07.las.switchcommgroup.com (66.209.64.178) [AS 23005] 84 msec 84 msec 88 msec
13 acs-wireless.demarc.switchcommgroup.com (66.209.64.70) [AS 23005] 88 msec 88 msec 88 msec
```

Pro srovnání

Originální síť:

```
  2 12.87.94.9 [AS 7018] 8 msec 8 msec 4 msec
  3 tbr1.cgcil.ip.att.net (12.122.99.38) [AS 7018] 8 msec 8 msec 8 msec
  4 12.122.99.17 [AS 7018] 8 msec 4 msec 8 msec
  5 12.86.156.10 [AS 7018] 12 msec 8 msec 4 msec
  6 tge1-3.fr4.sjc.llnw.net (69.28.171.66) [AS 22822] 68 msec 56 msec 68 msec
  7 ve5.fr3.sjc.llnw.net (69.28.171.209) [AS 22822] 56 msec 68 msec 56 msec
  8 tge1-1.fr4.lax.llnw.net (69.28.171.117) [AS 22822] 64 msec 64 msec 72 msec
  9 tge2-4.fr3.las.llnw.net (69.28.172.85) [AS 22822] 68 msec 72 msec 72 msec
 10 switch.ge3-1.fr3.las.llnw.net (208.111.176.2) [AS 22822] 60 msec 60 msec 60 msec
 11 gig5-1.esw03.las.switchcommgroup.com (66.209.64.186) [AS 23005] 60 msec 60 msec 60 msec
 12 66.209.64.85 [AS 23005] 64 msec 60 msec 60 msec
 13 gig0-2.esw07.las.switchcommgroup.com (66.209.64.178) [AS 23005] 60 msec 64 msec 60 msec
 14 acs-wireless.demarc.switchcommgroup.com (66.209.64.70) [AS 23005] 60 msec 60 msec 60 msec
```

Unesená síť:

```
  2 12.87.94.9 [AS 7018] 8 msec 8 msec 4 msec
 3 tbr1.cgcil.ip.att.net (12.122.99.38) [AS 7018] 4 msec 8 msec 8 msec
 4 ggr2.cgcil.ip.att.net (12.123.6.29) [AS 7018] 4 msec 8 msec 4 msec
 5 192.205.35.42 [AS 7018] 8 msec 4 msec 8 msec
 6 cr2-loopback.chd.savvis.net (208.172.2.71) [AS 3561] 16 msec 12 msec *
 7 cr2-pos-0-0-5-0.NewYork.savvis.net (204.70.192.110) [AS 3561] 28 msec 32 msec 32 msec
 8 204.70.196.70 [AS 3561] 28 msec 32 msec 32 msec
 9 208.175.194.10 [AS 3561] 32 msec 32 msec 32 msec
10 gig5-1.esw03.las.switchcommgroup.com (66.209.64.186) [AS 23005] 88 msec 88 msec 84 msec
11 66.209.64.85 [AS 23005] 88 msec 88 msec 88 msec
12 gig0-2.esw07.las.switchcommgroup.com (66.209.64.178) [AS 23005] 84 msec 84 msec 88 msec
13 acs-wireless.demarc.switchcommgroup.com (66.209.64.70) [AS 23005] 88 msec 88 msec 88 msec
```

Závěry

- Můžeme unést libovolný prefix, aniž by se cokoli rozbilo
- Můžeme ho unést skoro neviditelně
- AS_PATH nám útočníka neodhalí
- Filtrujte své zákazníky!
  - I před jimi samými

Výhledy do bezpečnosti BGP

- S-BGP – mrtvý standard
- soBGP – mrtvý standard
- Certifikace zdrojů @ RIPE
- Secure Inter-Domain Routing WG @ IETF

Zdroje

- http://www.ripe.net/ripe/tf/index.html
- http://tools.ietf.org/wg/sidr/
- http://www.networkworld.com/news/2009/011509-bgp-attacks.html
- http://web.mit.edu/net-security/Camp/2003/DBowie_IP_Hijacking.pdf
- https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf