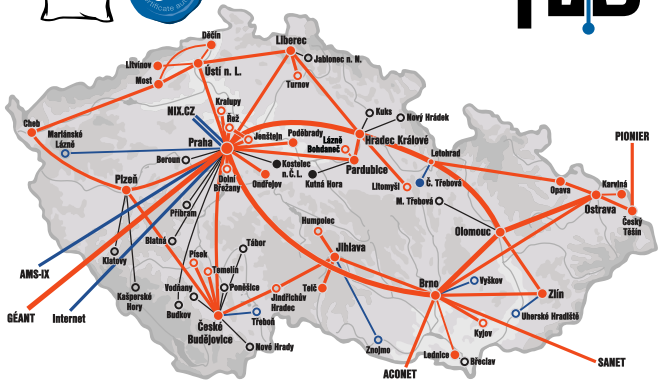
# DoS útoky v síti CESNET2

Ondřej Caletka

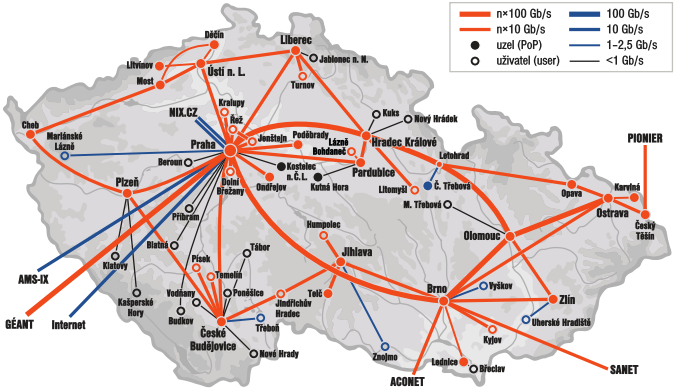

31. května 2016

# O sdružení CESNET



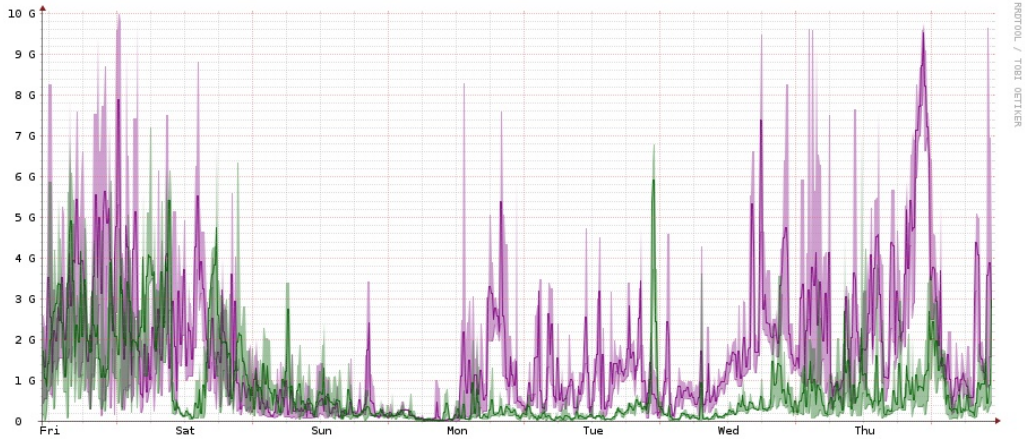
# Specifické podmínky NRENu

- dostatečně dimenzovaná páteřní síť
- velká variabilita legitimního provozu
- **žádné filtrování**[1]




[1] kromě povinných (BCP 38) či vyžádaných klientem

# Typický týdenní provoz



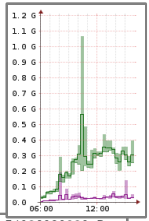
# Fenomén DoS

- zábava teenagerů
  - útrácení kapesného za (D)DoS-as-a-Service
  - cílem zejména herní a TeamSpeak servery spolužáků
  - velký problém pro provozovatele VPS
- hacktivismus
  - rozbíjení nepopulárních služeb
  - předpověď DoSů v blízké budoucnosti:
    - systém elektronické evidence tržeb
    - stránky MF ČR se seznamem blokovaných internetových stránek
- krátké trvání útoků (méně než pět minut)
  - často nedetekované monitoringem
  - zásadním způsobem naruší real-time služby
  - lidé si dnes všímají rychleji než monitoring

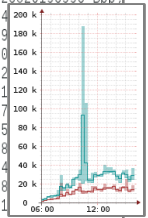
# Příklad krátkodobého zaplavení UDP pakety

```
Notification                : UDP from external networks and port 0,53,123,161 to internal IPS,
bytes>=1024, targets - DETECTED traffic anomaly
Detected                    : 195.113.[redacted] (dest. IP) - found 878 (limit 250) flows within
period of 5 seconds

Flows time range [GMT]      : 15/12/17 09:33:02-15/12/17 09:34:03
Flows time range [local]    : 15/12/17 10:33:02-15/12/17 10:34:03
```




```
50.241.253.129  udp(17)/0  --> 195.113.[redacted]  udp(17)/0 :  6113015 B,   5436 p, 1124.54286239882 Bpp,
186.215.207.138 udp(17)/0  --> 195.113.[redacted]  udp(17)/0 :  4732764 B,   4694 p, 1008.25820195995 Bpp,
46.188.59.141   udp(17)/0  --> 195.113.[redacted]  udp(17)/0 :  1576588 B,   1330 p, 1185.4[redacted]
61.85.1.79      udp(17)/0  --> 195.113.[redacted]  udp(17)/0 :  3466937 B,   3132 p, 1106.9[redacted]
202.114.238.116 udp(17)/0  --> 195.113.[redacted]  udp(17)/0 : 13477647 B,  11460 p, 1176.0[redacted]
117.102.65.174  udp(17)/0  --> 195.113.[redacted]  udp(17)/0 :  9227596 B,   7946 p, 1161.2[redacted]
217.128.111.66  udp(17)/0  --> 195.113.[redacted]  udp(17)/0 :   367793 B,    331 p, 1111.1[redacted]
219.222.224.6   udp(17)/0  --> 195.113.[redacted]  udp(17)/0 : 13262153 B,  11194 p, 1184.7[redacted]
163.29.216.61   udp(17)/0  --> 195.113.[redacted]  udp(17)/0 :  4589202 B,   4038 p, 1136.5[redacted]
96.90.226.11    udp(17)/0  --> 195.113.[redacted]  udp(17)/0 :  2143761 B,   2038 p, 1051.8[redacted]
112.160.7.249   udp(17)/0  --> 195.113.[redacted]  udp(17)/0 :   952083 B,    819 p, 1162.4[redacted]
219.223.18.20   udp(17)/0  --> 195.113.[redacted]  udp(17)/0 : 13569874 B,  11424 p, 1187.8[redacted]
123.57.177.192  udp(17)/0  --> 195.113.[redacted]  udp(17)/0 :  2836849 B,   2499 p, 1135.1[redacted]
218.244.142.146 udp(17)/0  --> 195.113.[redacted]  udp(17)/0 :   749959 B,    688 p, 1090.05668604651 Bpp,
24.111.41.107   udp(17)/0  --> 195.113.[redacted]  udp(17)/0 :  5840435 B,   5325 p, 1096.79530516432 Bpp,
187.141.38.238  udp(17)/0  --> 195.113.[redacted]  udp(17)/0 :   620221 B,    479 p, 1294.82463465553 Bpp,
```



# Trendy v (D)DoS

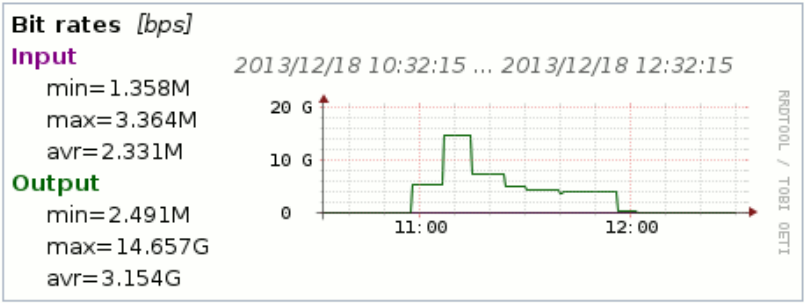
- použití bezespojových protokolů, často v kombinaci s falšováním zdrojových adres a odrazným/zesilujícím útokem
  - TCP SYN flood
  - DNS
  - NTP
  - SNMP
  - SSDP
- DNS dotazy na náhodné subdomény
  - použití ORR v kombinaci s botnetem nebo falšováním zdrojových adres
  - cílem je přetížit autoritativní servery daného doménového jména
  - zpětný rozptyl na rekurzivní resolvery

# Proč operátoři neimplementují BCP 38?

- čím blíže ke koncové síti, tím je to snazší
- jednoduchý `urpf-check` nefunguje při multihomingu
- výrobci síťových prvků často stále nepodporují automatické filtrování kompatibilní s multihomingem (Feasible Reverse Path Forwarding – BCP 84)
- uvolněná kontrola RPF-`loose` je neúčinná
- naše řešení: ACL na zákaznických portech
  - ručně spravované
  - náchylné na chyby
  - nejspíše příliš nákladné pro většinu ISP

# Zkušenosti s DoS v síti CESNET2

- klientský router ohlašuje /16, ale pouze /17 je dále zpracováno
  - pakety do zbývajících /17 se vrací zpět do páteře
  - klientská linka je přetížena
- souhrný tok při útoku dokáže snadno zahltit 10Gbps přípojku

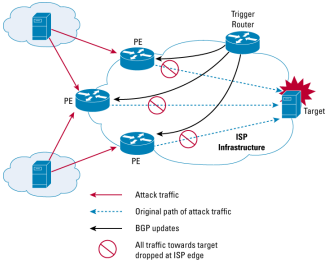


# Přijatá protiopatření

- RTBH pro klienty
  - útoky míří na malé množství IP adres
  - zahození provozu již v páteři brání přetížení klientské linky
  - připravujeme jemnější RTBH založené na BGP Flowspec
- omezení rychlosti určitých protokolů na vnějším perimetru sítě
  - pro bezespojové protokoly jako NTP, SNMP,...
  - typický NTP provoz ~2 Mbps
  - různé velikosti paketů pro normální provoz a pro útok
- omezení rychlosti DNS odpovědí pro různě sítě
  - samostatné fronty pro skupinu /16
  - včetně omezení četnosti IP fragmetů (!)

# Remotely triggered black hole filtering

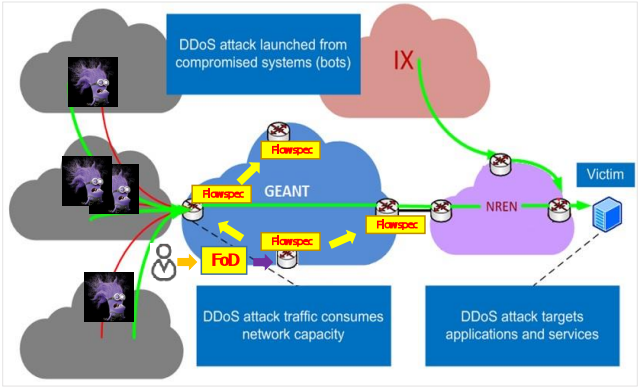
- distribuce směrovacích pravidel protokolem BGP
- směrování nežádoucího provozu do černé díry hned u zdroje
- místo zahození možno přesměrovat na IPFIX sondu k analýze
- možnost redistribuce pravidel do Tier-1 (TeliaSonera)
- povinné v rámci klubu FENIX




Zdroj: Cisco

# GÉANT Firewall-on-demand

- služba provozovatele panevropské akademické páteře
- každý NREN může nastavovat pravidla pro své adresy
- pravidla jsou aplikována v celé páteři




Zdroj: GÉANT

# Unwanted Traffic Removal Service

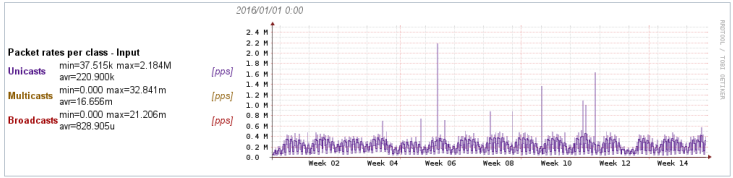
- komunitní služba zajišťovaná organizací Team Cymru
- centrální BGP route server
- operátoři jeho prostřednictvím sdílí adresy, na které si nepřejí přijímat provoz
- participující operátoři zahazují provoz pro dané adresy už ve své síti

UTRS

Unwanted Traffic Removal Service

20 1996–2016 CESNET

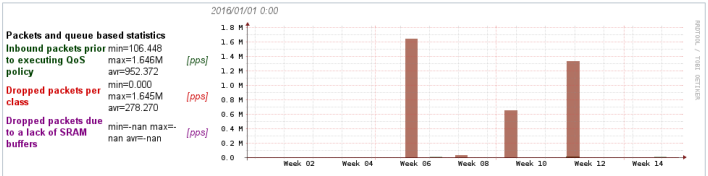
# Praktické nasazení QoS – NTP





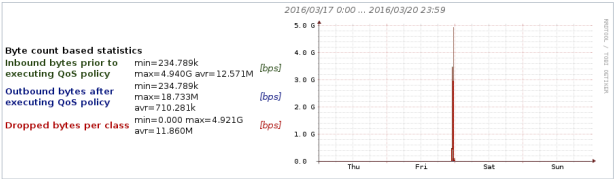
[QoS]

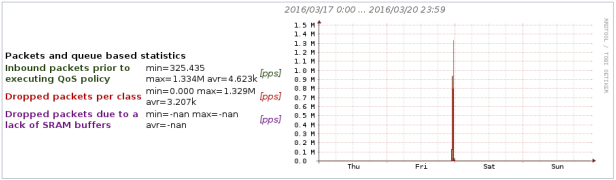
[classmap] 'Policy-NTP' (matchAny)

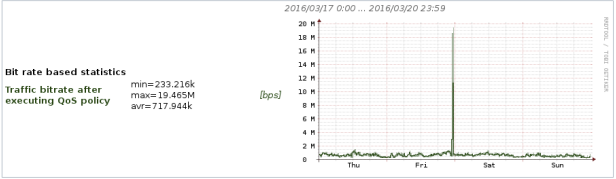



- ukázka z reálného 10GbE rozhraní za 4 měsíce
- v době útoku saturováno NTP pakety
- QoS pravidlo zahazuje pouze v době útoku

# Praktické nasazení QoS – NTP – detail




- detail jednoho útoku
- zdrojový tok 4 Gbps
- po aplikaci QoS výstupní tok 20 Mbps

# Příklad zesilujícího útoku pomocí DNS

## nula v čísle portu označuje IP fragmenty

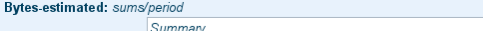
| 0 | Src-IP | Dst-IP | Protocol | Src-Port | Dst-Port | Flow-Start [CEST] | Flow-End [CEST] | Bytes-measured | Pkts-measured | Avr-Pkt-Length |
|---|---|---|---|---|---|---|---|---|---|---|
| 1. | 1.4.157.31 | 195.113.x.x | udp (17) | 0 | 0 | 16/03/17 05:44:13.193 | 16/03/17 05:48:44.764 | 6.460 MB | 5.134 kp | 1319.47 |
| 2. | 1.4.157.31 | 195.113.x.x | udp (17) | domain (53) | 4444 | 16/03/17 05:44:24.243 | 16/03/17 05:48:41.764 | 4.989 MB | 3.506 kp | 1492 |
| 3. | 1.21.11.29 | 195.113.x.x | udp (17) | 0 | 0 | 16/03/17 05:44:49.167 | 16/03/17 05:47:44.582 | 3.522 MB | 2.750 kp | 1343.03 |
| 4. | 1.21.11.29 | 195.113.x.x | udp (17) | domain (53) | 52670 | 16/03/17 05:47:02.155 | 16/03/17 05:47:02.155 | 1.418 KB | 1.000 p | 1452 |
| 5. | 1.21.11.62 | 195.113.x.x | udp (17) | 0 | 0 | 16/03/17 05:45:36.179 | 16/03/17 05:47:42.753 | 2.563 MB | 2.003 kp | 1341.93 |
| 6. | 1.21.11.62 | 195.113.x.x | udp (17) | domain (53) | 55838 | 16/03/17 05:47:01.276 | 16/03/17 05:47:01.290 | 18.434 KB | 13.000 p | 1452 |
| 7. | 1.21.56.104 | 195.113.x.x | udp (17) | 0 | 0 | 16/03/17 05:44:47.254 | 16/03/17 05:47:43.131 | 2.866 MB | 2.236 kp | 1343.99 |
| 8. | 1.36.15.238 | 195.113.x.x | udp (17) | 0 | 0 | 16/03/17 05:46:56.947 | 16/03/17 05:47:07.083 | 29.899 KB | 22.000 p | 1391.68 |
| 9. | 1.36.15.238 | 195.113.x.x | udp (17) | domain (53) | 4841 | 16/03/17 05:47:04.056 | 16/03/17 05:47:04.076 | 2.883 KB | 2.000 p | 1476 |
| 10. | 1.36.81.9 | 195.113.x.x | udp (17) | 0 | 0 | 16/03/17 05:46:54.931 | 16/03/17 05:47:04.856 | 51.634 KB | 39.000 p | 1355.72 |
| 11. | 1.36.81.9 | 195.113.x.x | udp (17) | domain (53) | 4444 | 16/03/17 05:46:57.477 | 16/03/17 05:47:06.080 | 24.504 KB | 17.000 p | 1476 |
| 12. | 1.36.81.9 | 195.113.x.x | udp (17) | domain (53) | 6800 | 16/03/17 05:47:03.878 | 16/03/17 05:47:03.878 | 1.441 KB | 1.000 p | 1476 |
| 13. | 1.36.81.9 | 195.113.x.x | udp (17) | domain (53) | 9733 | 16/03/17 05:47:00.895 | 16/03/17 05:47:00.895 | 1.441 KB | 1.000 p | 1476 |
| 14. | 1.36.81.9 | 195.113.x.x | udp (17) | domain (53) | 34344 | 16/03/17 05:47:02.202 | 16/03/17 05:47:02.214 | 2.883 KB | 2.000 p | 1476 |
| 15. | 1.55.240.156 | 195.113.x.x | udp (17) | 0 | 0 | 16/03/17 05:45:16.285 | 16/03/17 05:47:43.074 | 1.600 MB | 1.256 kp | 1335.79 |
| 16. | 1.55.247.236 | 195.113.x.x | udp (17) | 0 | 0 | 16/03/17 05:44:47.234 | 16/03/17 05:47:43.032 | 1.278 MB | 1.007 kp | 1330.66 |
| 17. | 1.55.247.236 | 195.113.x.x | udp (17) | domain (53) | 35600 | 16/03/17 05:47:01.242 | 16/03/17 05:47:01.277 | 8.789 KB | 6.000 p | 1500 |
| 18. | 1.64.40.35 | 195.113.x.x | udp (17) | 0 | 0 | 16/03/17 05:46:51.207 | 16/03/17 05:47:13.996 | 52.222 KB | 40.000 p | 1336.88 |
| 19. | 1.64.40.35 | 195.113.x.x | udp (17) | domain (53) | 22723 | 16/03/17 05:47:01.819 | 16/03/17 05:47:01.819 | 1.441 KB | 1.000 p | 1476 |
| 20. | 1.64.161.49 | 195.113.x.x | udp (17) | 0 | 0 | 16/03/17 05:46:57.999 | 16/03/17 05:47:08.444 | 15.345 KB | 12.000 p | 1309.42 |
| 21. | 1.64.161.49 | 195.113.x.x | udp (17) | domain (53) | 25745 | 16/03/17 05:47:02.349 | 16/03/17 05:47:02.349 | 1.457 KB | 1.000 p | 1492 |
| 22. | 1.64.168.108 | 195.113.x.x | udp (17) | 0 | 0 | 16/03/17 05:46:55.811 | 16/03/17 05:47:05.931 | 45.126 KB | 34.000 p | 1359.09 |
| 23. | 1.64.168.108 | 195.113.x.x | udp (17) | domain (53) | 4444 | 16/03/17 05:46:53.971 | 16/03/17 05:47:04.865 | 23.062 KB | 16.000 p | 1476 |
| 24. | 1.179.131.145 | 195.113.x.x | udp (17) | 0 | 0 | 16/03/17 05:45:00.162 | 16/03/17 05:47:45.017 | 2.905 MB | 2.286 kp | 1332.53 |
| 25. | 1.179.136.166 | 195.113.x.x | udp (17) | 0 | 0 | 16/03/17 05:44:53.154 | 16/03/17 05:49:53.986 | 0.368 MB | 0.282 kp | 1367.35 |
| 26. | 1.179.136.166 | 195.113.x.x | udp (17) | domain (53) | 4444 | 16/03/17 05:44:29.195 | 16/03/17 05:49:11.972 | 1.917 MB | 1.340 kp | 1500 |
| 27. | 1.179.138.90 | 195.113.x.x | udp (17) | 0 | 0 | 16/03/17 05:45:06.188 | 16/03/17 05:47:43.639 | 3.100 MB | 2.436 kp | 1334.27 |
| 28. | 1.179.141.231 | 195.113.x.x | udp (17) | 0 | 0 | 16/03/17 05:46:21.179 | 16/03/17 05:47:43.610 | 1.571 MB | 1.247 kp | 1321.38 |

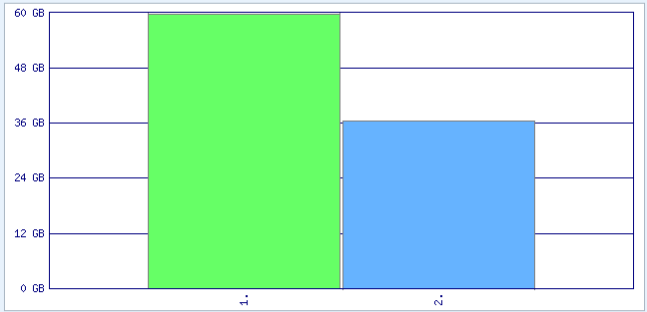
# Fragmentovaný provoz během zesilujícího útoku

**Bytes-estimated:** *sums/period*

*Summary*

| | | |
|---|---|---|
| **In graph** | 96.227 GB | 100.00% |
| **Rest of results** | 0.000 GB | NA |
| **Total** | 96.227 GB | 100.00% |






| | Protocol | Src-Port | Flow-Start | Flow-End | Bytes-estimated |
|---|---|---|---|---|---|
| 1. > | udp (17) | 0 | 16/03/17 05:42:50.184 | 16/03/17 05:49:59.926 | 59.783 GB |
| 2. > | udp (17) | domain (53) | 16/03/17 05:42:51.195 | 16/03/17 05:49:59.616 | 36.444 GB |

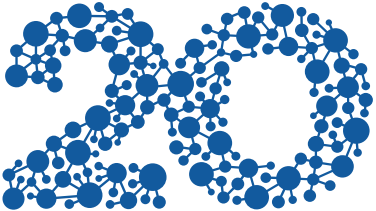
1996–2016 CESNET

# Závěr

- DoS útoky jsou stále častějším jevem
  - a bude hůře...
  - krátké trvání komplikuje manuální zmírňování
  - budoucnost patří automatizovaným proti-DoS opatřením
- síťový hardware stále nepodporuje některé klíčové funkce
  - požadujte *Feasible Reverse Path Forwarding – BCP 84* při příští obměně hardwaru
- podporujme komunity jako FENIX
  - sdílení zkušeností
  - vzájemná výpomoc
  - autoregulace místo regulace
  - **osobní důvěra**

# Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://Ondřej.Caletka.cz



1996–2016
CESNET
SPOLUPRÁCE
VÝZKUM
KOMUNITA