The bridge to possible

POLISH NETWORK OPERATORS GROUP

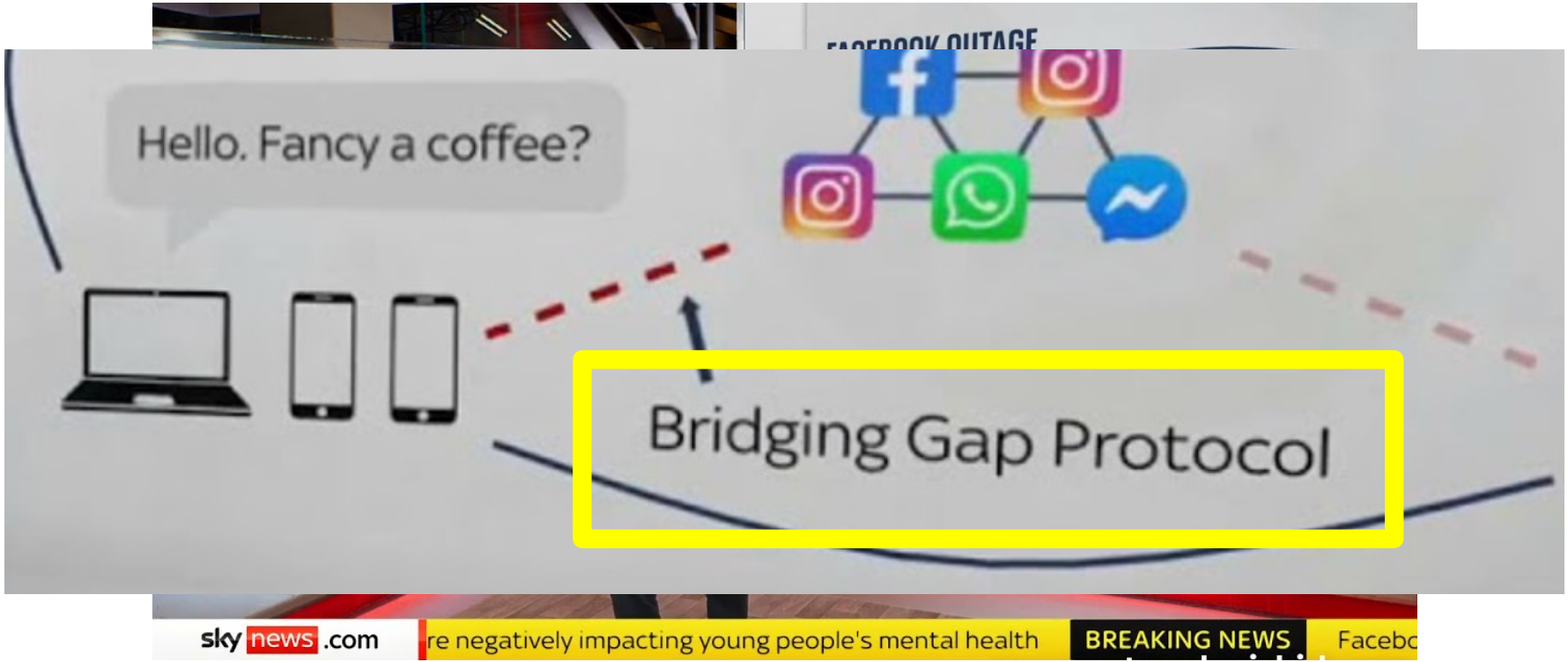
Jak przechwytywać ruch w Internecie

(for fun & profit)

Łukasz Bromirski / https://lukasz.bromirski.net / @LukaszBromirski

PLNOG 2022.09

Chyba nikt nie ma wątpliwości...



Chyba nikt nie ma wątpliwości...

https://ripe84.ripe.net/wp-content/uploads/presentations/36-Cloudflare-Anatomy-of-a-Route-Leak-RIPE84-1.pdf

Od 2018 zrobiło się naprawdę poważnie
Całe państwa zaczynają bawić się bez rękawiczek

- China Unicom wszedł do ekosystemu kontynentalnych Stanów Zjednoczonych w wielu miastach
  - Miało to sens – np. duża ilość chińczyków w USA
- Następnie (w 2018 na masową skalę) zaczęli aktywnie “pomagać” Chińskiej Partii Komunistycznej przechwytując ruch z dużych amerykańskich korporacji oraz trzyliterowych agencji
- USA FCC zdecydowała o usunięciu licencji China Unicom oraz nakazała usunięcie w terminie 30 dni całej infrastruktury
- Chiny używają od tego czasu infrastruktury w innych krajach do tego samego

2018 Attack Ranking by Country

Country	Attack Distribution
China	85.63%
Barbados	5.04%
Antigua	4.18%
Guyana	0.81%
Switzerland	0.75%

2018 Ranking by Source Operator

Network Operator	Attack Distribution
China Unicom	81.15%
Flow Barbados	5.64%
Cable & Wireless Antigua	4.68%
China Mobile	1.93%
Orange Caraibe Guyana	0.91%

2019 Attack Ranking by Country

Country	Attack Distribution
Barbados	28.10%
Antigua	18.70%
Mexico	12.92%
Switzerland	6.01%
British Virgin Islands	4.22%

2019 Ranking by Source Operator

Network Operator	Attack Distribution
Flow Barbados	29.04%
Cable & Wireless Antigua	19.33%
Telcel Mexico	8.56%
Swisscom Switzerland	6.21%
Telefonica Movistar	4.80%

4. China reduced its attack volumes, favoring more targeted espionage, likely using proxy networks in the Caribbean and Africa to conduct its attacks, having close ties in both trade and technology investment.

Źródła:
https://docs.fcc.gov/public/attachments/FCC-21-37A1.pdf
https://img1.wsimg.com/blobby/go/cda61771-2b5c-4a41-aac5-0bd319d1fe07/downloads/Far-From-Home_Intel-RP_2018-2019_B.pdf

“Mali gracze” też to robią – cały czas

- 8 sierpień, 2021: Pakistani Telecom (ponownie!) AS17557 “porywa” prefiks T-Mobile (172.50.49/24)

- Rosja celuje w Ukraine (mocno):
  - NETGROUP, RU AS35004 porywa 31.148.149/24 & 95.47.59.0/24 należące do AS212463 NGROUP, UA
- Polska jest atakowana przez chińskie kraje proxy – głównie Brazylię, ale również (!) Ukrainę:
  - ENTEL CHILE AS27651 porywa 193.107.216/24 z SKYTECH AS201814
  - BIGNET AS43668 porywa 185.242/22 z IP Services AS34907

Źródła:
https://arstechnica.com/information-technology/2019/06/bgp-mishap-sends-european-mobile-traffic-through-china-telecom-for-2-hours
https://www.zdnet.com/article/russian-telco-hijacks-internet-traffic-for-google-aws-cloudflare-and-others/
https://portal.bgpmon.net/data/12389_apr2020.txt

Mali, duzi, wszyscy...

Cisco BGPStream @bgps... · 25/08/2022

BGP,HJ,hijacked prefix AS7941 207.241.224.0/21, INTERNET-ARCHIVE, US,-,By AS39171 GW-AS Centrum Uslug Informatycznych, PL, bgpstream.com/event/295665

1

Jeszcze o uderzeniu Federacji Rosyjskiej

May 29
Kherson stayed connected to the global internet even after Russian forces took control in March.

June 1
Then the connection closed. Russian authorities rerouted Kherson's internet traffic through a state-controlled network in Crimea.

June 5
Russia has only added to the network infrastructure, routing more traffic through Moscow to strengthen its control of Kherson's internet.

Więcej:
https://www.wired.com/story/ukraine-russia-internet-takeover/
https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html
https://www.kentik.com/blog/rerouting-of-kherson-follows-familiar-gameplan/

Quiz #1 – ASNy zarezerwowane przez IANA to...

A) 0, 112, 23456, 64495-65551, 4200000000-4294967294

B) 0, 112, 23456, 64496-65551, 4200000000-4294967295

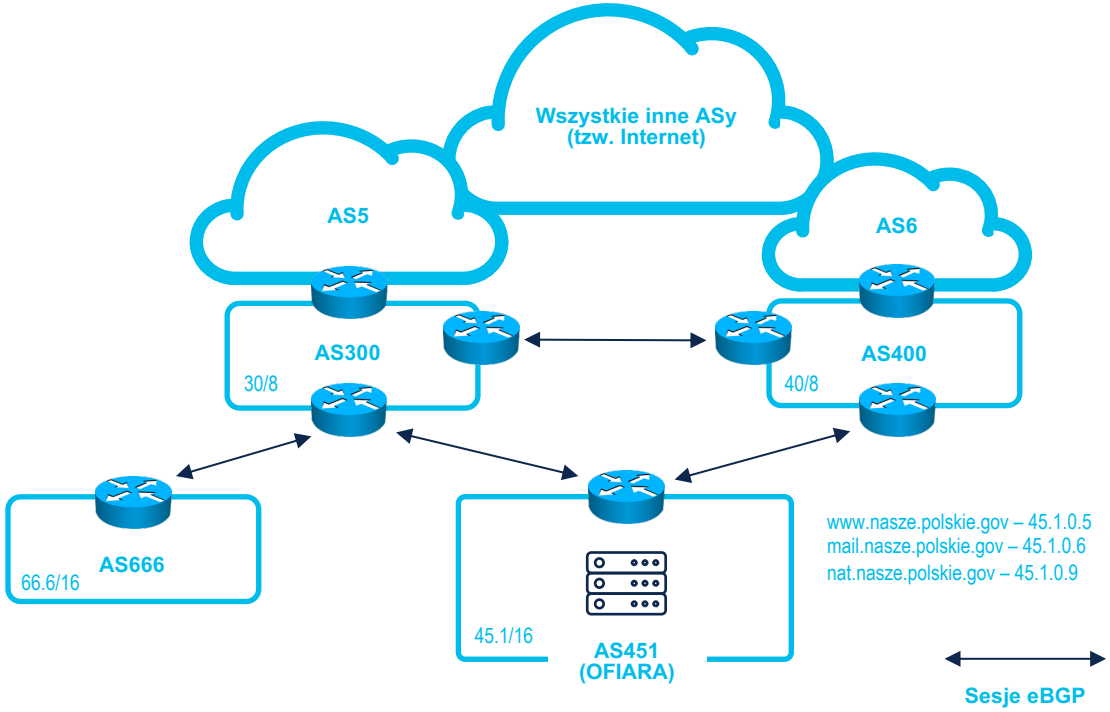
C) 0, 112, 23456, 64496-65551, 4200000000-4294967295

D) 0, 112, 23456, 64496-64534, 4200000000-4294967295

Opis problemu

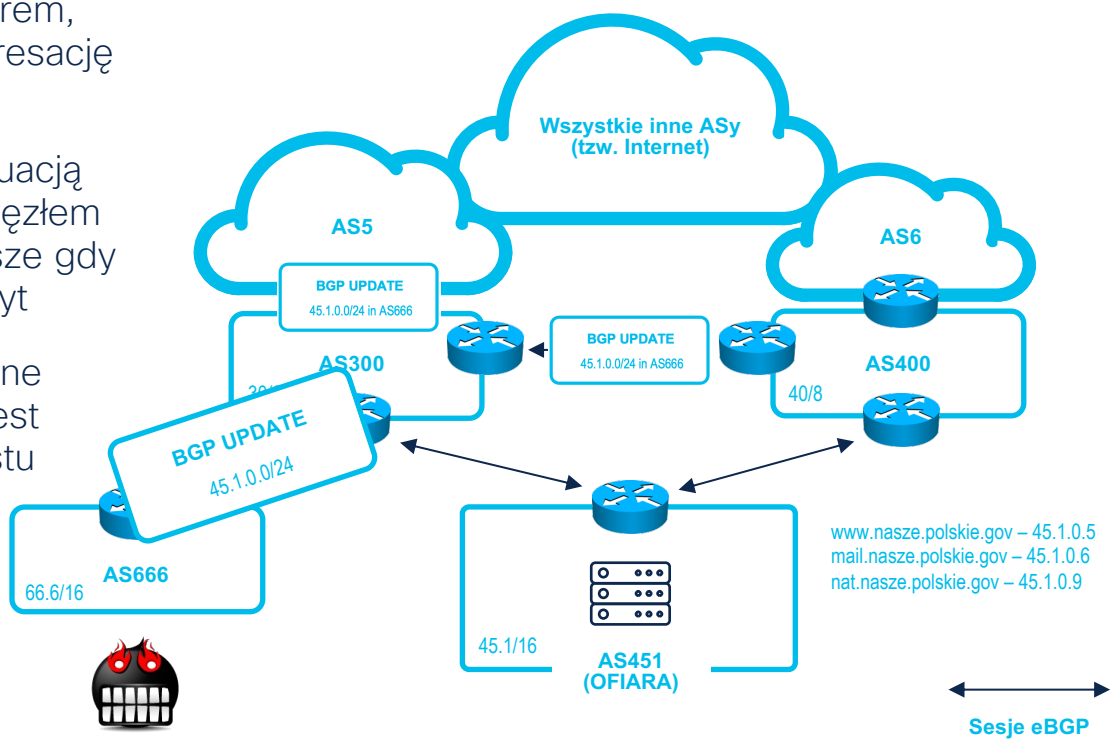
Internet to sieć połączonych ASów

- System Autonomiczny (AS) BGP należy do firm, instytucji rządowych czy w ogólności podmiotów posiadających zasoby internetowe
- Każdy posiadający dostęp do internetu używa swojego, lub zasobów należących do któregoś z ASów
- Do niedawna, nikogo specjalnie nie interesowało kto przesyła jaki ruch, poza kwestiami finansowymi



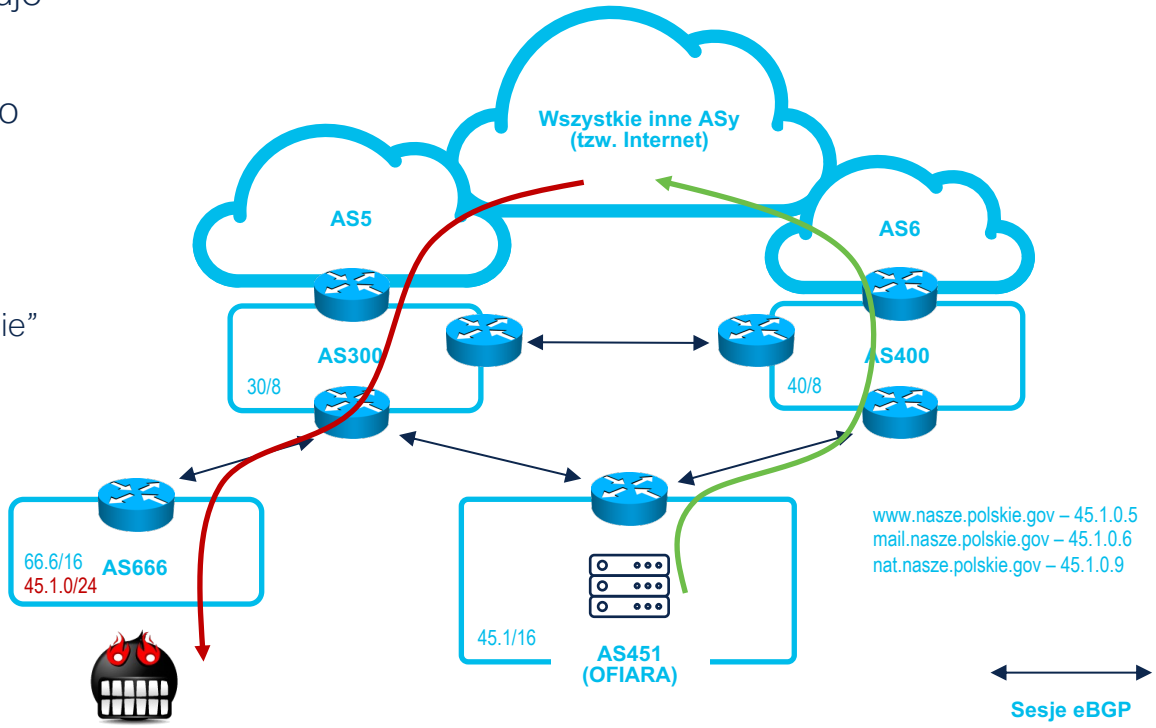
Internet to sieć połączonych ASów

- Oznacza to, że jeśli jestem złym aktorem, mogę zacząć podszywać się pod adresację przypisaną do Twojego ASu
- Filtry zabezpieczające przed taką sytuacją są proste do wdrożenia jeśli jesteś węzłem końcowym internetu, trochę trudniejsze gdy jesteś operatorem realizującym tranzyt
- ...do momentu, w którym ich poprawne stworzenie i utrzymanie na bieżąco jest prawie niemożliwe a czasem po prostu niepraktyczne/nieopłacalne



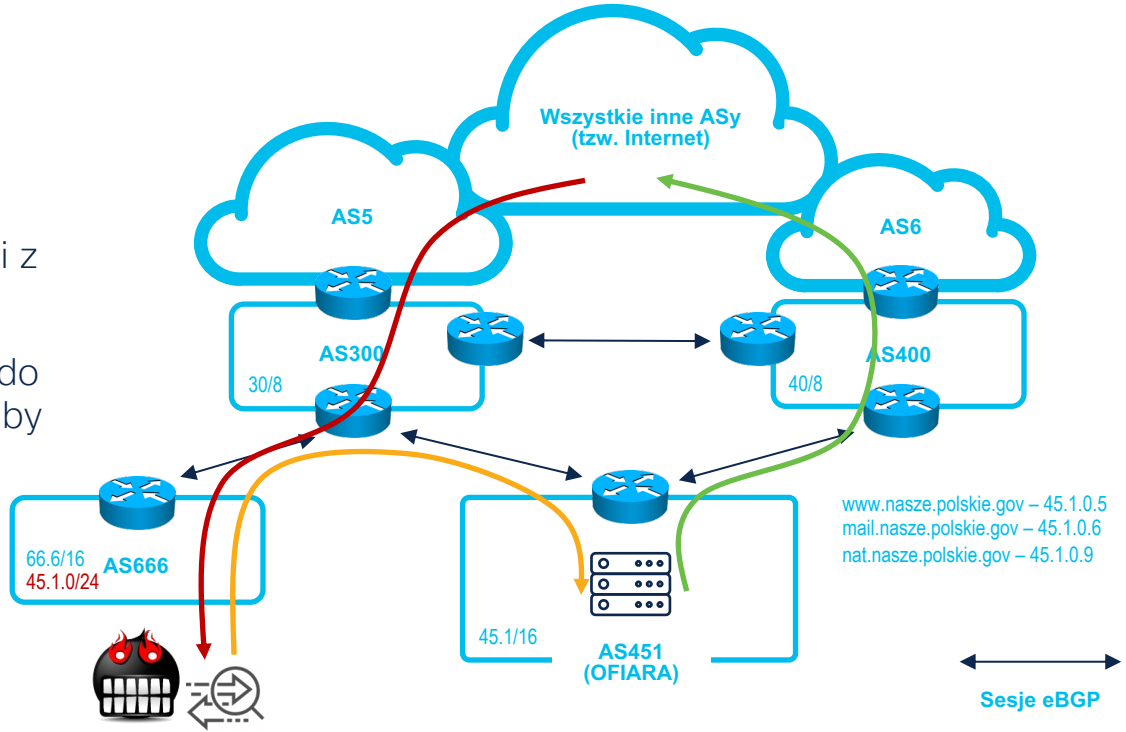
Internet to sieć połączonych ASów

- Ktoś za nat.nasze.polskie.gov inicjuje połączenie do internetu
- Ruch router po routerze zmierza do miejsca docelowego, ale ruch powrotny trafi do złego aktora
- Dlaczego?
  - Zły aktor już zainstalował “w internecie” dokładniejszy wpis na sieć ofiary:
  - 45.1/16 -> OFIARA
  - 45.1.0/24 -> ZŁY AKTOR



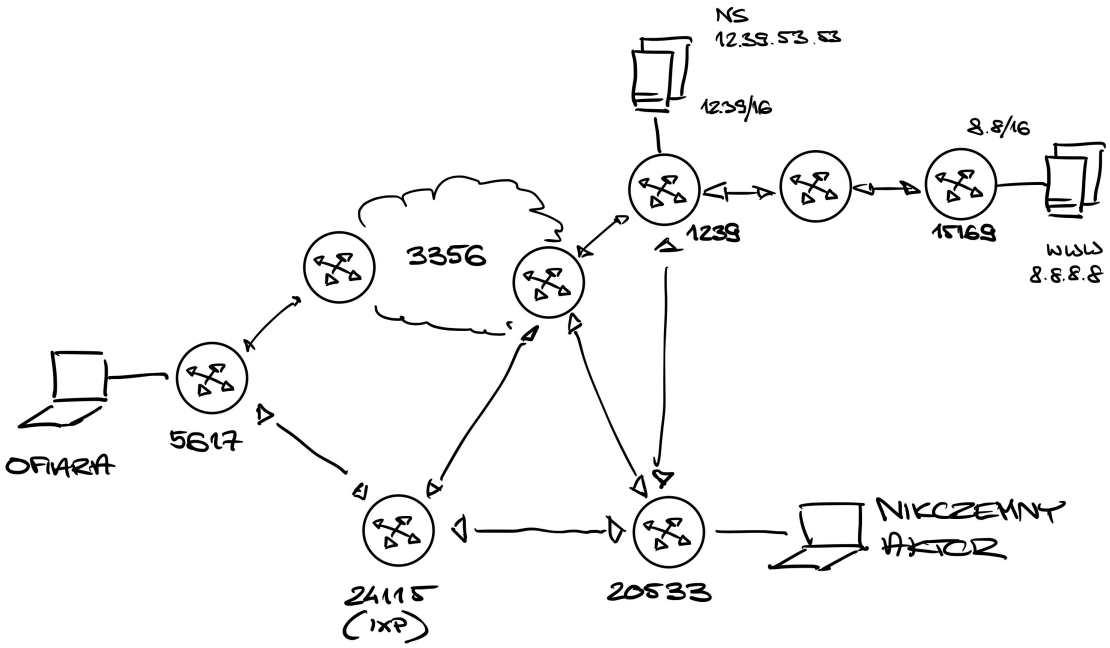
Internet to sieć połączonych ASów

- Tak prosty atak zwykle od razu zatrzyma większość komunikacji (TCP zwykle wymaga komunikacji dwukierunkowej)
- “Profesjonalny” zły aktor zadba również o “zatrucie” routingu usługi z której korzysta ofiara...
- ...oraz zadba o “zwrócenie” ruchu do jednego i drugiego podmiotu tak, aby do komunikacji w ogóle doszło

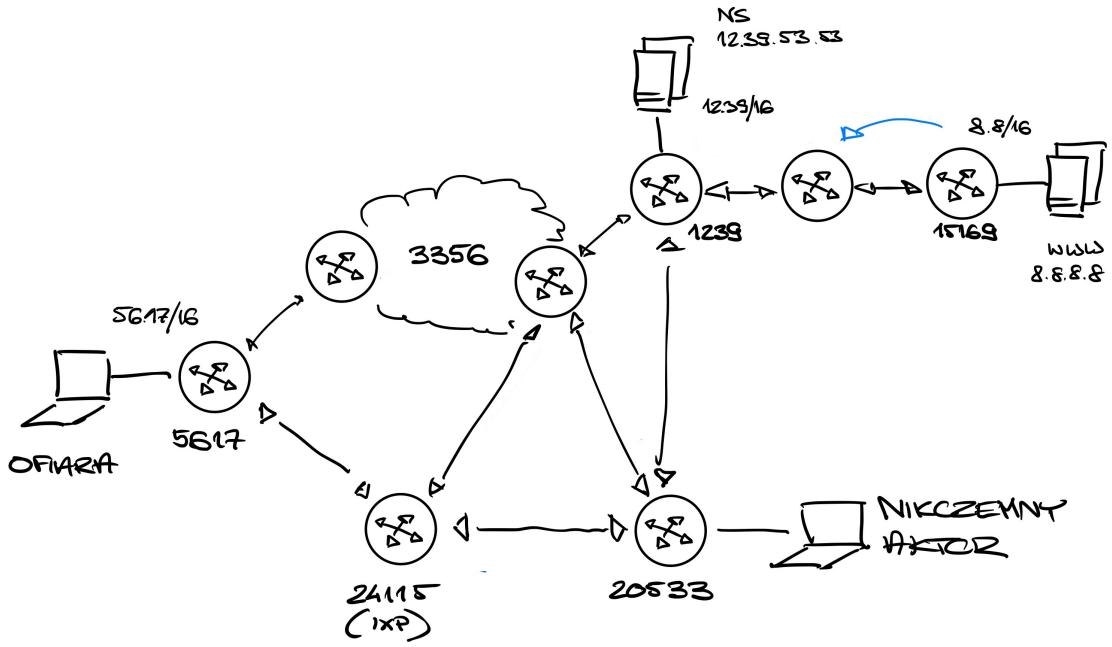


Problem na żywo

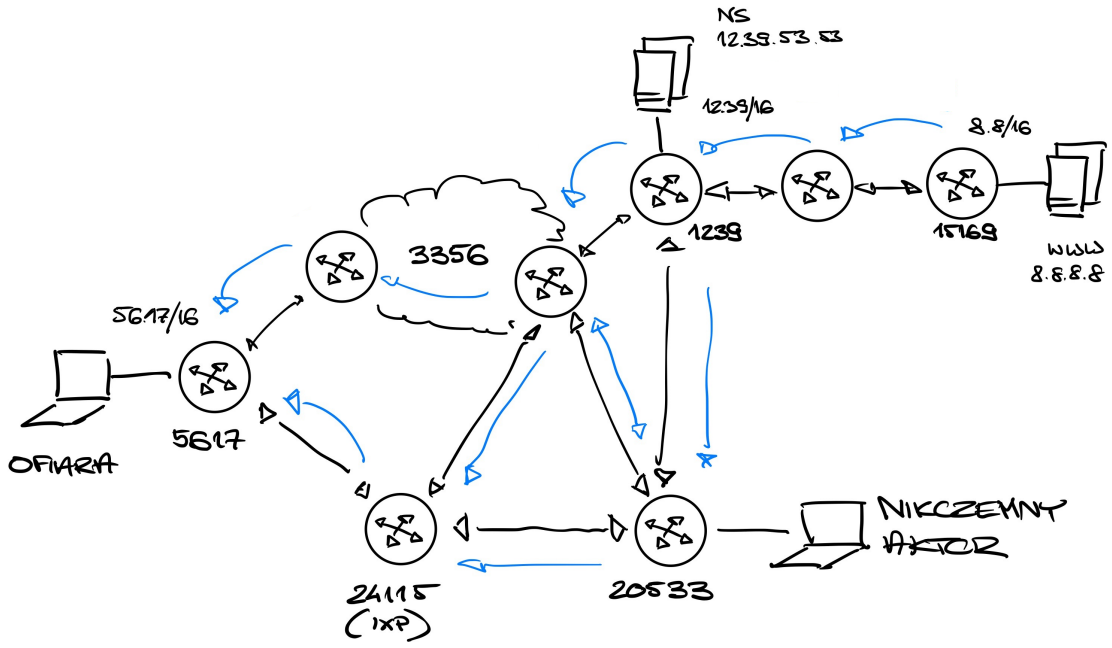
Nasz przykładowy internet
(można kupić w każdym sklepie z internetami)



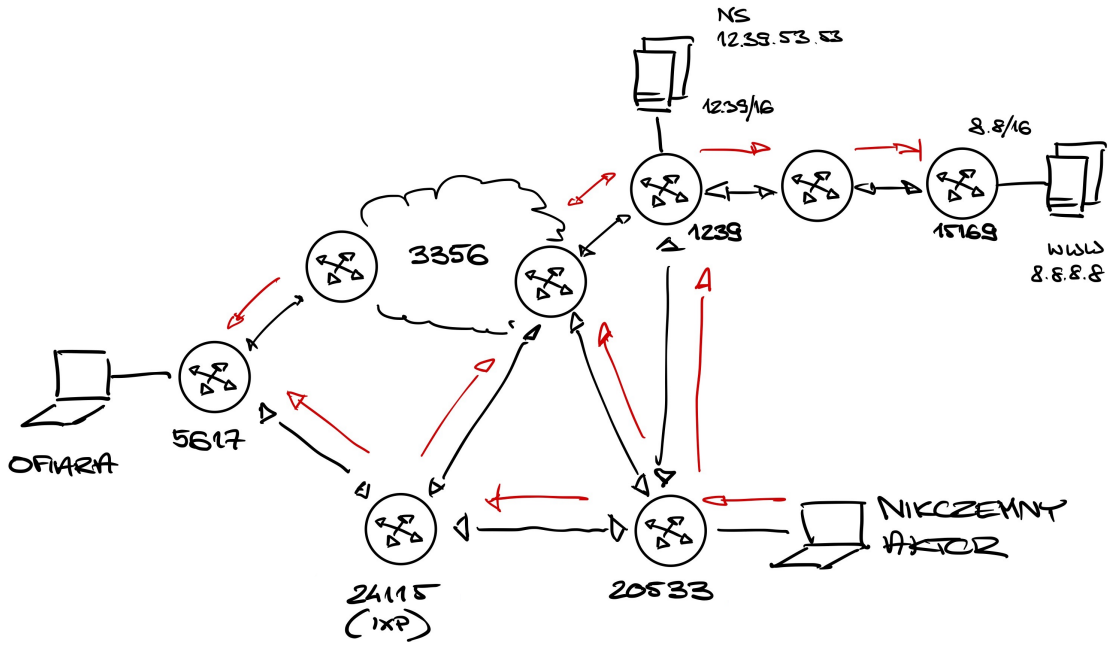
Jak Ofiara dostaje się do Usługi?
(skąd znamy trasę do 8.8/16?)



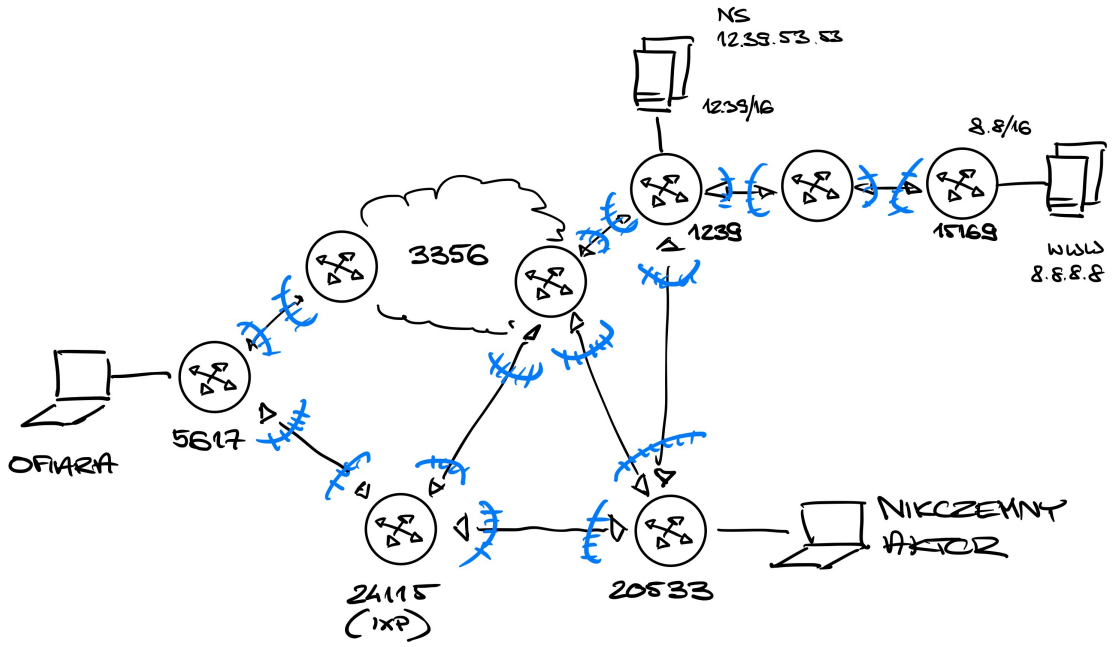
Jak Ofiara dostaje się do Usługi?
(56.17.10.100 do 8.8.8.8?)



Jak Nikczemny Aktor to zepsuje?
(rozgłaszając dokładniejszy prefiks – 8.8.8/24)



Jak będziemy się bronić?
(filtry, filtry, dużo filtrów)



Quiz #2 – RFC opisujące IP

- RFC 1918 opisuje bloki adresów IP prywatne
- RFC 5737 opisuje bloki adresów IP zarezerwowane dla dokumentacji

- ...które (nie)sławne RFC opisuje sposób testowania urządzeń sieciowych (routerów/przełączników), często wspominany w przetargach?

Jak się zabezpieczyć?

Jak się zabezpieczyć?

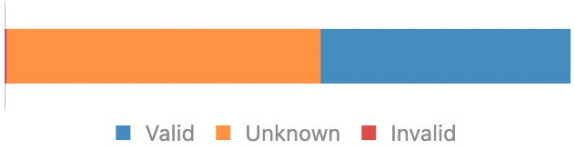
- Sensowne filtry ruchowe do swoich routerów BGP (179/tcp)
- Sensowne filtry dla BGP na sesji ingress i egress (RFC 8212!)
- Nałóż TCP-AO lub MD5 na sesje BGP
- BGP RPKI – i w przyszłości BGPsec
- wyższe warstwy - aplikacyjne:
  - DNSSEC
  - TLS 1.2+

Podsumowanie

Statystyki BGP RPKI dla Polski

Routing completeness (RPKI)

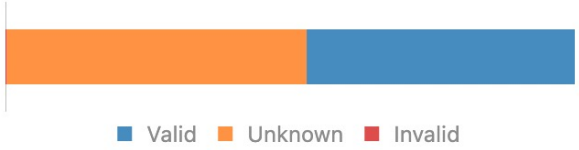
Valid	3,404	44.2%
Unknown	4,271	55.4%
Invalid	32	0.4%



Czerwiec 2022

Routing completeness (RPKI)

Valid	3,672	47.1%
Unknown	4,102	52.7%
Invalid	17	0.2%



Wrzesień 2022

Źródło:
https://observatory.manrs.org/#/overview

CISCO SECURE