Polisen

Carrier/ISP data in intelligence work

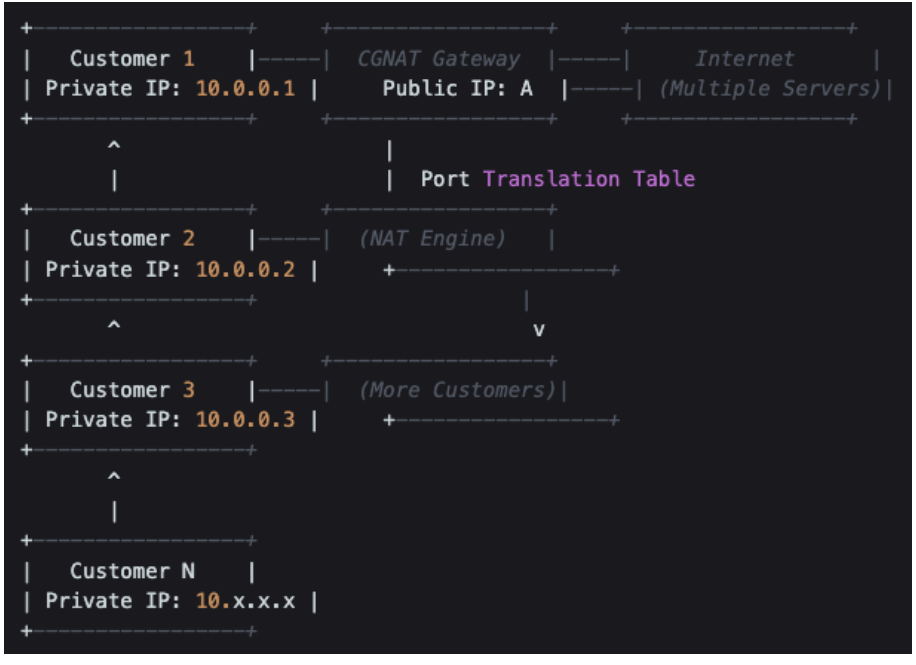
Swedish Police, Stockholm region

The state of crime prevention today

- Sweden’s gang violence has moved from regional acts of violence to crime/violence as a service (CaaS/VaaS)
- Intelligence work has moved from targeting people in the real world to aliases/users on chat platforms
- Anonymous aliases has made tying IP addresses to these aliases an important tool in the toolbox of identifying instigators of CaaS/VaaS

How IP addresses are used today

- When an IP address has been identified we send a request to the ISP or phone carrier for customer information
- We've typically sent requests for IPv4 addresses, necessitating precise date/time and also port number for phone users
- If we're lucky our target is easily identifiable amongst users on that IP address and port number at that particular time



Polisen

Differences in IPv4 vs IPv6 *for us*

- We’ve only really started to come across IPv6 over the past year, and have limited experience of it’s impact on our work

- As explained by carriers, the first block of eight in an IP address identifies the user, making identification uniquely precise

```
2001:0db8:0000:0000:0000:0000:1428:07ab/64
```

- Due to this, when it comes to phone carrier users, having coms based on IPv6 reduces uncertainty and makes us more efficient in combating violent crime in Sweden (and assisting neighbours)

Retrieving carrier/ISP data today

- Another component of our work is retrieving historical and live communication data for mobile phone users
- This carrier-supplied information gives us data on pinged cell towers, calls/texts, involved parties in coms, and more
- Triangulation of suspect location through cell tower triangulation works well today, but it’s not as precise as it could be

Existing but untapped potential today

- There is a part of mobile network communication that isn’t currently being used by Swedish operators (regarding historical customer data)

- This is an area we are looking into, but this might be an area where we would like to see a national directive to make our coms based crime prevention more effective
  - Norway as case study
  - Could have big implications for crime prevention and ER

To summarize

- A widespread use of IPv6, especially in cell phone networks, would greatly increase our efficiency and precision

- If this were to be combined with greater precision in historical location data for cell phone users our ability to efficiently combat today’s mobile suspects would be greatly improved