Council of the
European Union

Brussels, 16 January 2017
(OR. en)

5127/17

LIMITE

CYBER 7
COPEN 9
JAI 33
COSI 8
ENFOPOL 33

NOTE

From:	EUROPOL/EC3
To:	Delegations
Subject:	Carrier-Grade Network Address Translation (CGN) and the Going Dark Problem - initial debate

Delegations will find in Annex a discussion paper from Europol/EC3 dedicated to issues related to the Carrier-Grade Network Address Translation (CGN).

CARRIER-GRADE NETWORK ADDRESS TRANSLATION (CGN)

and

the Going Dark Problem

Recently, many new technologies have made the headlines because they hinder law enforcement's ability to follow criminal leads and attribute crime. But the *Going Dark* problem is not limited to the TOR network, proxy servers, bullet proof hosting and encrypted communication applications. A far more diffused technology - the carrier-grade network address translation (CGN) - is posing massive attribution problems to the law enforcement community around the world.

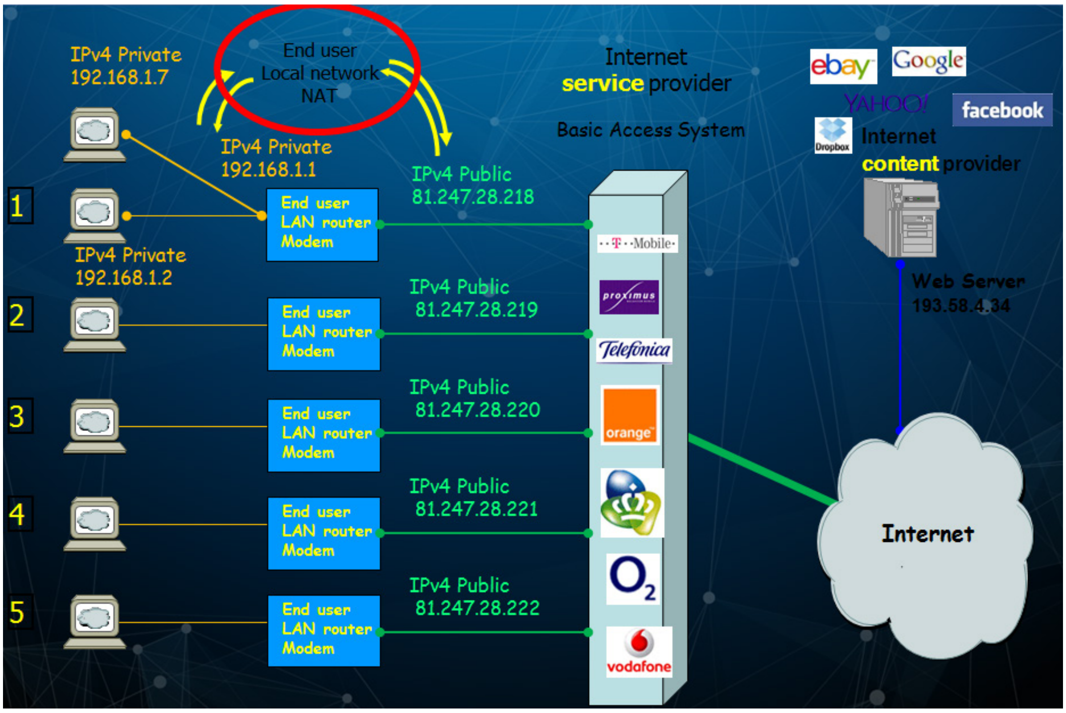
The Internet Service Providers (ISPs) and mobile Internet service providers have adopted the CGN as temporary solution to address the gradual exhaustion of Internet Protocol version 4 (IPv4) addresses resulted from the increased global demand for Internet accessibility. Although the newer version of Internet Protocol, known as IPv6, offers a virtually unlimited number of IP addresses, the transition from IPv4 to IPv6 has been slower than expected because of the lack of commercial incentive to do so and the numerous necessary upgrades to the IPv4 legacy infrastructure. The transition from IPv4 to IPv6 has forced many network operators and ISPs to support and maintain both address infrastructure schemes so that devices are able to run IPv4 and IPv6 in parallel (dual stack).

What is Carrier Grade NAT (CGN)?

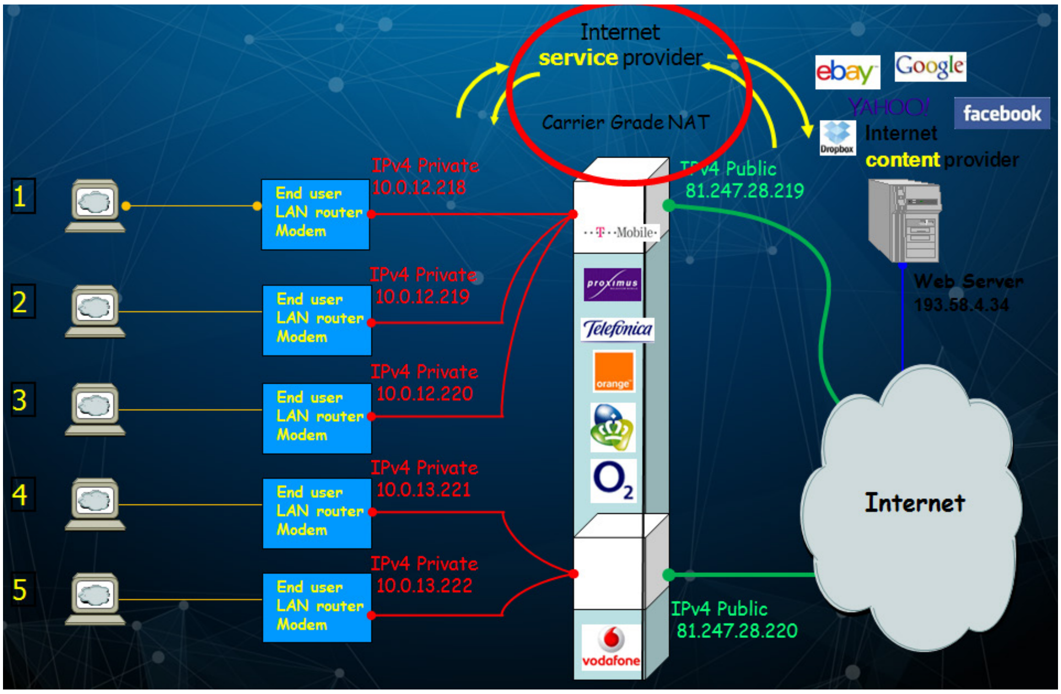
CGN is an evolution of the traditional Network Address Translation (NAT) protocol, which has been used for the last 25 years in private networks (home, small businesses). NAT dynamically translates a collection of private IP addresses connected to each of the home or business user's devices to one public IPv4 address used within one network (i.e. routable on the internet). CGN is much more pervasive than NAT; instead of an endpoint user having a single public IP address, CGN allows a single IP address to be shared by potentially thousands or hundreds of thousands of subscribers at the same time.

To illustrate:

IPv4-address attribution WITHOUT CGN:



IPv4-address attribution WITH CGN



CGN impact on Law Enforcement Investigations

With CGN, law enforcement has lost its ability to associate and link a particular cyber criminal's activity back to a particular IP address. Cyber investigators now need to determine which one of the hundreds or thousands of consumers associated with a particular public IP address is behind the actions which they are investigating.

One Member State reported that in a recent investigation into Child Sexual Exploitation Material (CSEM) distributed and hosted via a cloud-based service, the investigators had to investigate each one of the 50 clients using that public IP at this time in order to identify who was ultimately uploading the CSEM, because the cloud-based service provider did not log the relevant information to define which customer was using the public IP.

CGN technologies have therefore negative consequences in terms of data protection and privacy because law enforcement authorities must resort to far more privacy invasive investigative techniques to identify potential suspects.

Scale of the problem

A survey conducted in August 2016 among European cyber-investigators, shows that the problem of crime attribution related to CGN technologies is regularly encountered by 80% of the respondents during their investigations.

In a number of cases, the investigation is discontinued. Alternatively the investigations are delayed because the investigators needed to resort to additional, lengthy and more invasive investigative techniques in order to identify an end-user. 98% of the respondents support a European-wide mandatory legal requirement for electronic service providers to identify end-users of an IP address.

Future threats and developments

Originally CGN has been used to palliate the shortage of IPv4 addresses. Consequently, for many years, most actors involved shared the view that the simplest solution to this problem was to wait for the full transition to IPv6, because the trillions of IPv6 addresses available would eliminate the need to use CGN.

However, current trends indicate that the transition to IPv6 will not be completed before at least the next two decades and the use of CGNs by network operators is increasing by the day. According to a recent a survey carried out among 70 traditional ISPs (cable, fiber and ADSL) worldwide, 38% of these traditional ISPs have CGN in place and 12% are planning to deploy it[1]. The situation is even worse for GSM providers: according to the same study, 95% of mobile ISPs (i.e. IP addresses provided by GSM providers) use CGN technologies.

The impact on investigations is significant: one Member State reported that in more than 50% of criminal investigations, IP addresses used by criminals were mobile IPs (smartphone) and that in 90% of these cases those mobile IP addresses were operated behind a CGN and could not be attributed.

In addition, responding to customers’ demand, telecom equipment companies such as CISCO and JUNIPER have started selling software solutions that provide CGNs for networks fully operating IPv6[2].

This means that CGN is here to stay and that the old policy response (i.e. wait for the transition to IPv6) is not the right approach from the perspective of the victims. The use of CGN will continue to grow in spite of the transition to IPv6, further impeding the law enforcement ability to perform a trace back to an individual end-user of an IP address.

[1] A Multi-perspective Analysis of Carrier-Grade NAT Deployment¸ ACM IMC 2016

[2] https://www.netflask.net/nat66-and-ipv6-ula/

Solution and way forward

- In order to be able to trace back an individual end-user to an IP address on a network using CGN, law enforcement must request additional information[3] from content providers via legal process:

    - Source and Destination IP addresses;
    - Exact time of the connection (within a second);
    - **Source port number.**

  However, the lack of harmonized data retention standard requirements in Europe[4] means that content service, Internet service and data hosting providers are under no legal obligation to retain this type of information, meaning that even a more elaborate request from LEA would not yield useable information from the provider.

  Regulatory/legislative changes would be helpful to ensure that content service providers systematically retain the necessary additional data (source port) information to allow law enforcement and judicial authorities to identify one specific end-user among the thousands of users sharing the same public IP address.

- As some content providers in Europe do store the relevant information but some others do not practical solutions can be sought through collaboration between the electronic/Internet? service providers and law enforcement using already established channels for cooperation such as the EU Internet Forum.

[3] Internet Engineering Task Force (IETF) Recommendation for Comment (RFC) 6302, June 2011 - “Logging Recommendations for Internet-Facing Servers” https://tools.ietf.org/html/rfc6302 .

[4] On 8 April 2014 the European Court of Justice annulled the Data Retention Directive http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

The latter could provide an excellent platform for discussion with the most important ISPs/content providers the need to implement the traceability of source port numbers and to provide these numbers on a voluntary basis when requested (directly or by legal process) by law enforcement and judiciary authorities in order to facilitate the attribution of crime.

<u>Question:</u>

Would Member States support such approach and thus recommend an extension of the scope of the EU Internet Forum to also cover the issue of CGN?

- On 31st January 2017 a **<u>European Network of law enforcement specialists in CGN</u>** will be established, the secretariat of which will be established/provided by? at Europol. The aim of this network is to:
  - document cases of non-attribution linked to CGN in EU,
  - document existing best practices to overcome CGN-related attribution problems currently in place in some Member States,
  - raise awareness of European policy-makers about the problem of attribution linked to CGN technologies,
  - represent the voice of law enforcement developing a common narrative and advocating for a voluntary scheme at EU level to improve traceability by engaging in a coordinated fashion with ISPs and content providers.

<u>Question:</u>

How would Member States suggest the results of the work and the eventual recommendations of the future network of law enforcement specialists in CGN be brought to the attention of policy-makers and at which level in order to ensure their implementation, including by the providers and by this to facilitate the attribution of crime?