CLOSING THE ONLINE CRIME ATTRIBUTION GAP: EUROPEAN LAW ENFORCEMENT TACKLES CARRIER-GRADE NAT (CGN)

02Feb2017

Press Release

European Network of Law Enforcement Specialists on CGN created at Europol to address a little known but major capability gap in law enforcement's attempts to identify offenders online.

On 31 January 2017, a meeting of European law enforcement cybercrime specialists was held at Europol's headquarters in The Hague. This meeting addressed the increasing problem of non-crime attribution associated with the widespread use of Carrier-Grade Network Address Translation (CGN) technologies by internet service providers (ISPs). The meeting included presentations from industry experts, to broaden law enforcement understanding of the way in which internet service providers (providing access to the internet) and electronic content providers (websites and communication platforms) operate with regards to CGN.

CGN technologies are used by ISPs to share one single IP address among multiple subscribers at the same time. As the number of subscribers sharing a single IP has increased in recent years –in some cases several thousand – it has become technically impossible for ISPs to comply with legal orders to identify individual subscribers. In most EU countries, when served with a legal order, these

providers have a legal obligation to provide subscriber information on a person suspected of involvement in criminal activities. The impact of this technological development on police work is considerable. An increasing proportion of investigations into terrorism and serious crime rely on the ability to identify offenders via a capability that is now being seriously eroded.

CGN technologies have been used by ISPs for a number of years as a solution to postpone the necessary financial investments to upgrade their networks to allow for the transition to the next generation of Internet Protocol Address version 6, or IPv6, which offers an unlimited pool of IP addresses. Due to the undeniable benefits of IPv6 over IPv4, this transition to IPv6 is called upon by the vast majority of internet engineering experts, governments, international organisations (including the UN and the EU), but also NGOs promoting a safe, open and secure internet[1].

European Network of Law Enforcement Specialists on CGN

The difficulties of online crime attribution related to CGN have been reported by law enforcement around Europe for a number of years. Europol raised the issues in the Internet Organised Crime Threat Assessment (IOCTA) in 2014 and 2016.

The law enforcement community is alarmed by the widespread and growing use of CGN technologies by ISPs. A recent study showed that in 2016, 90% of mobile internet network operators (GSM providers) and 38% of fixed line internet access providers (cable, fibre and ADSL) are using CGN technologies, while 12% are planning to deploy it in the coming months[2].

A study conducted by Europol in the summer of 2016 showed that the scale of the online crime-attribution problems stemming from the use of CGN is significant. 80% of the European cybercrime investigators surveyed had encountered problems in their investigations relating to the use of CGN, causing them to be either delayed or stopped. These cases concern investigations of serious offences, such as online child sexual exploitation, arms trafficking and terrorist propaganda.

Because the issue is increasing, Europol took the initiative to launch the **European Network of Law Enforcement Specialists on CGN**. The network will systematically document cases of non-attribution related to CGN, share existing best practices to overcome CGN-related attribution problems and contribute to engaging with ISPs and content providers to improve the traceability of IP addresses behind CGN.

Europol's Director Rob Wainwright said: *"CGN technology has created a serious online capability gap in law enforcement efforts to investigate and attribute crime. It is particularly alarming that individuals who are using mobile phones to connect to the internet to facilitate criminal activities cannot be identified because 90% of mobile internet access providers have adopted a technology which prevents*

them from complying with their legal obligations to identify individual subscribers. On behalf of the European law enforcement community Europol is actively exploring ways to address this urgent problem with stakeholders in the EU and Industry."

Steven Wilson, Head of Europol's European Cybercrime Centre, added: *"Ensuring EU law enforcement investigations are effective and result in the arrests of responsible parties is one of Europol's key functions. The issues relating to CGN, specifically the non-attribution of malicious groups and individuals, should be resolved. I am convinced that the European Network of Law Enforcement Specialists on CGN will help to voice the concerns of the law enforcement community with EU decision-makers."*

[1] ISOC, IETF, RIPE NCC, ICANN etc.

[2] A Multi-perspective Analysis of Carrier-Grade NAT Deployment, ACM IMC 2016

CRIME AREAS

Cybercrime

TARGET GROUPS

General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other

ENTITIES

European Cybercrime Center (EC3)

Source URL: https://www.europol.europa.eu/newsroom/news/closing-online-crime-attribution-gap-european-law-enforcement-tackles-carrier-grade-nat-cgn