EUROPOL

ARE YOU SHARING THE SAME IP ADDRESS AS A CRIMINAL? LAW ENFORCEMENT CALL FOR THE END OF CARRIER GRADE NAT (CGN) TO INCREASE ACCOUNTABILITY ONLINE

17 Oct 2017

Press Release

Europol and the Estonian Presidency of the EU Council address the serious online capability gap in law enforcement efforts to investigate and attribute crime created by CGN technologies.

On 13 October 2017, the Estonian Presidency of the Council of the EU and Europol held a workshop attended by 35 EU policy-makers and law enforcement officials, to address the increasing problem of non-crime attribution associated with the widespread use of Carrier Grade Network Address Translation (CGN) technologies by companies that provide access to the internet. The workshop was supported by experts from Europol's partners: Proximus, CISCO, ISOC, the IPv6 Company, and the European Commission.

CGN technologies are used by internet service providers 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 internet service providers to comply with legal orders to identify individual subscribers. This is relevant as in criminal investigations an IP address is often the only information that can link a crime to an individual. It might mean that individuals cannot be distinguished by their IP addresses anymore, which may lead to innocent individuals being wrongly investigated by law enforcement because they share their IP address with several thousand others – potentially including criminals.

The Estonian EU Presidency identified the issue of CGN and online crime attribution as one of its priorities and will table the results of the workshop on the agenda of the Standing Committee on Operational Cooperation on Internal Security (COSI) as a contribution to improving the EU´s cybersecurity.

The inability to identify internet subscribers on the basis of an IP address has put the European judiciary and law enforcement communities in a difficult and complex situation, creating a public safety gap and putting the privacy of citizens at risk because it forces judiciary and law enforcement authorities to investigate many more individuals than would normally be necessary. Every crime for which a connected device is used can be affected: terrorism, cybercrime, drug trafficking, online child sexual exploitation, facilitated illegal immigration, murder or fraud, and all EU Member States are affected.

Europol’s Executive Director Rob Wainwright: *"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 grateful to the Estonian Presidency of the EU Council for 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."*

Workshop participants, supported by industry experts, reviewed criminal investigations which failed because of CGN. Furthermore, existing technical and policy solutions were discussed that could be adopted at European level such as a voluntary code of conduct for Internet access providers to reduce the use of CGN and the number of subscribers behind each IP address. Other solutions reviewed were the possibility for electronic content providers to log source port numbers, or the possibility to adopt regulations for the internet industry to increase IPv6 deployment.

The EU and its Member States have started to address the online capability gap created by CGN technologies. In June 2017 the UK and France adopted an Action Plan on Internet and Terrorism, which includes a call to address the CGN online crime attribution problem. The European Union

Cybercrime Task Force (heads of cybercrime units from law enforcement agencies across the 28 EU Member States), adopted a joint declaration in July 2017 to warn about the negative impact of CGN technologies on online crime attribution. More recently, the European Commission has set out policy responses in the Joint Communication adopted on 13 September 2017 on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU". The European Parliament expressed concerns that the use of CGN technologies by Internet access providers seriously hampers investigations in a resolution adopted on 3 October 2017.

What are CGNs?

On the internet, every connected device needs an IP address. However, the number of IP addresses (Internet Protocol Version 4) is limited and insufficient to meet the exploding demand for new addresses for connected devices including connected objects and smart phones. A new version of IP address (IPv6) which provides an unlimited number of IP addresses is available but the transition from IPv4 to IPv6 requires Internet access providers and internet content providers (websites, social media, webmail services, etc.) to update software and hardware. To address this problem, Internet access providers adopted CGN technologies which allow sharing of IPv4 addresses with multiple internet users (several thousands). This was supposed to be a temporary solution until the transition to IPv6 was completed but for some operators it has become a substitute for the IPv6 transition. Despite IPv6 being available for more than 5 years the internet access industry increasingly uses CGN technologies (90% for mobile internet and 50% for fixed line) instead of adopting the new standard.

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/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end-of-carrier-grade-nat-cgn-to-increase-accountability-online