Cybercrime Digest

Bi-weekly update and global outlook by the
Cybercrime Programme Office of the Council of Europe (C-PROC)

16-31 October 2017

Source: Europol

Date: 17 Oct 2017

Are you sharing the same IP address as a criminal? LEAs call for the end of carrier grade nat (CGN) to increase accountability online

"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." READ MORE

Source: Independent

Date: 19 Oct 2017

Internet giants attend G7 summit for first time as world takes fight to extremists online

"The world's major internet companies are attending a G7 summit for the first time, in an urgent attempt to draw up tough new rules to counter the dramatic rise in the use of social media by terrorists. These talks with multinationals at the meeting, which began today in Italy, come amid deep concern that the volume of Islamist traffic on tech platforms will increase even more, as Isis tries to compensate for its defeat in Syria and Iraq by instigating attacks in the West online." READ MORE

Source: isBuzzNews

Date: 27 Oct 2017

Amnesty's Turkish Chair on Trial in Post-Coup Crackdown-Over Allegations He Downloaded ByLock App

"It has been reported that the chair of Amnesty International in Turkey and 10 other Amnesty activists have gone on trial in Istanbul in one of the most high-profile tests of Turkish criminal law since the failed coup in 2016 led to tens of thousands of arrests and dismissals from public office. Taner Kılıç, chair of Amnesty in Turkey since 2014, is on trial on two separate charges, largely on the basis of allegations that he downloaded a widely available phone messaging application called ByLock." READ MORE

Source: Lexology

Date: 24 Oct 2017

ICANN under pressure over GDPR preparations, as future of WHOIS is mired in uncertainty

"The Global Data Protection Regulation (GDPR), adopted in 2016, becomes enforceable on May 25 2018 uniformly across the European Union. The aim of the regulation is to protect EU citizens and residents from privacy and data breaches, and it therefore requires explicit consent to be obtained for the collection – and use, including publication – of personal data. Crucially, while an EU regulation, it applies to all companies processing and holding the personal data of subjects residing in the EU, regardless of the company's location. Therefore, ICANN (the Internet Corporation for Assigned Names and Numbers) and non-EU registries and registrars are impacted. For ICANN, the GDPR is set to have a significant impact on WHOIS, with the organisation acknowledging: "Since GDPR will likely effect how WHOIS data is displayed, it could impact our ability to maintain a single global WHOIS system. In turn, this will likely impact either ICANN's agreements or its ability to enforce contractual compliance of its agreements using a single and consistent approach." In short, on the face of it, the GDPR could result in WHOIS as we know it coming to an end. […] The use of WHOIS data to investigate fraud, consumer deception, intellectual property violations, or other violations of law could qualify as a legitimate interest, although this would have to be weighed against the rights and freedoms of the data subject." READ MORE

Source: Reuters

Date: 16 Oct 2017

U.S. Supreme Court to decide major Microsoft email privacy fight

"The U.S. Supreme Court on Monday agreed to resolve a major privacy dispute between the Justice Department and Microsoft Corp (MSFT.O) over whether prosecutors should get access to emails stored on company servers overseas. The justices will hear the Trump administration's appeal of a lower court's ruling last year preventing federal prosecutors from obtaining emails stored in Microsoft computer servers in Dublin, Ireland in a drug trafficking investigation. That decision by the New York-based 2nd U.S. Court of Appeals marked a victory for privacy advocates and technology companies that increasingly offer cloud computing services in which data is stored remotely. Prosecutors say a ruling in favor of Microsoft could undermine a range of criminal investigations." READ MORE

Source: Engadget

Date: 16 Oct 2017

Telegram fined after refusing to provide user data to Russia

"Back in June, Russia asked the messaging app Telegram to hand over confidential user data because it claimed terrorists have been using the service to plan attacks. This week the Meshchansky Court of Moscow fined Telegram 800,000 rubles (the equivalent of about $14,000) for failure to provide the Russian government with decryption keys to user messages. It's not an outright ban, which is what Russia threatened Telegram with, and the size of the fine implies that Russia's doing this for show. Telegram founder Pavel Durov posted about the decision on the social networking site VK (which he also founded). He claims that the demands of the FSB, Russia's state security organization, are unconstitutional. What's more, they are not feasible from a technological standpoint." READ MORE

Source: The Washington Post

Date: 24 Oct 2017

Russia is pushing to control cyberspace. We should all be worried.

"A draft of a Russian proposal for a new "United Nations Convention on Cooperation in Combating Information Crimes" was recently shown to me by a security expert who obtained a copy. The 54-page document includes 72 proposed articles, covering collection of Internet traffic by authorities, "codes of conduct" for cyberspace and "joint investigation" of malicious activity. The language sounds bureaucratic and harmless, but experts say that if adopted, it would allow Russia to squeeze cyberspace even more. […] The Moscow daily reported that the Russian Foreign Ministry had described the convention as an "innovative" and "universal" attempt to replace the 2001 Budapest Convention, which has been signed by the United States and 55 other countries but rejected by Russia." READ MORE

Source: GhanaWeb

Date: 25 Oct 2017

"I'll equip security agencies to fight cybercrime", President of Ghana declares government plans

"President Nana Addo Dankwa Akufo-Addo has declared plans by the government to roll out some policies which will see to the equipping of the country's law enforcement agencies, and the training of crime officers to enable them address issues of cyber-crime. The President, speaking at the opening of the National Cyber-Security Week, and the inauguration of the National Cyber-Security Inter-Ministerial Advisory Council, mentioned the training of all involved in the arrest and prosecution of criminals as high on his government's agenda. [...] The National Cyber Security Adviser, Albert Antwi-Boasiko, revealed at a media encounter that the document for the ratification of the Convention on Cybercrime, also known as the Budapest Convention, would be completed by the end of the year." READ MORE

RELATED ARTICLES

GhanaWeb, Government to partner Facebook, Google against cybercrime, 23 Oct 2017

Source: Prospectiva en Justicia y Desarrollo

Date: 24 Oct 2017

El gobierno de Colombia presenta un proyecto al Congreso para adherirse al Convenio de Budapest

"El Gobierno nacional radicó ante el Congreso de la República un proyecto de ley que busca la adhesión del Estado colombiano al Convenio Internacional de Budapest que busca la cooperación internacional entre los Estados para intensificar la lucha judicial contra la cibercriminalidad trasnacional. En buena hora Colombia inicia los pasos para acoger el Convenio de Budapest pues el desarrollo de las tecnologías de la información ha facilitado que organizaciones al margen de la ley cometan delitos informáticos que afectan la vida y la integridad de las personas, la libertad e integridad sexual y la seguridad de las naciones. […] Gran parte de estos crímenes no son investigados y los responsables solo son sancionados con instrumentos legales locales, por eso se hace necesaria la cooperación internacional para la investigación de estos crímenes." READ MORE

Source: First 5000

Date: 27 Oct 2017

Supporting cyber-security boosts Australian – Sri Lankan trade

"Sri Lanka's efforts to join international partners in tackling cyber-crime offer a shining example to other nations and have helped secure conditions for Australian trade. The Council of Europe Convention on Cybercrime, known as the Budapest Convention […] has had an enormous impact over the years and is now considered the de facto legal standard for legislation on cybercrime and electronic evidence around the world. It has been adopted by both Australia and Sri Lanka in recent years and now underpins mutual cyber-security between the two nations, bolstering a 70-year commercial relationship worth $1 billion a year. […] Australian businesses looking to trade with their Sri Lankan counterparts can now be assured that the Sri Lankan criminal justice system mirrors Australian legislative and procedural laws. Australian and Sri Lankan businesses share consistent safety and security standards and AUSCERT and SLCERT, the cyber security agencies in each country, cooperate closely on an even playing field." READ MORE

Source: CIOmag

Date: 27 Oct 2017

Cybercriminalité : le Maroc ciblé par le groupe arabe de cyber-espionnage « Faucons du désert »

"Le groupe arabe de cyber-espionnage, « Faucons du désert », a ciblé, récemment, pas moins de 179 sites électroniques au Maroc. Parmi ces sites, figurent ceux de plusieurs établissements publics. Les comptes privés de plusieurs politiques et ambassadeurs ont de même été piratés. A en croire le rapport de l'éditeur d'antivirus russe Kaspersky sur l'Afrique du Nord pour l'année 2017 et repris par *le360.ma* en partant d'informations du quotidien Al Akhbar, cette cyberattaque massive a été perpétrée récemment, mais aucune précision sur la période." READ MORE

Source: The Japan Times

Date: 17 Oct 2017

Child sex abuse rising with internet use in Southeast Asia

"Rising internet use in Southeast Asia is fueling the spread of material that is abusive and sexually exploitative of children, particularly as growing numbers of young people put footage of themselves online, an Australian police expert said on Tuesday. […] "The big problem we're seeing at the moment is the proliferation of self-produced material by children. It's just killing us," said Jon Rouse, a member of "Taskforce Argos," an Australian police unit that targets online child sex abuse networks, referring to children livestreaming themselves, whether at the instigation of a sex offender or a friend. "That material then gets used by sex offenders against them."In a seven-day check on Bangkok, more than 3,600 individual internet addresses had been identified sharing child exploitation material, said Rouse, who was speaking on the sidelines of a conference in the Thai capital." READ MORE

Source: GIZMODO

Date: 16 Oct 2017

Australia Launches First Nation-Wide Reporting System for Revenge Porn

"Victims of revenge porn – the nonconsensual distribution of explicit images – have a difficult path to navigate to regain their privacy and seek justice. The laws have yet to catch up to the crime, and the average person doesn't have the means to quickly take down intimate images from the web – they're often at the mercy of tech giants. But the Australian government is trying to address the issue with a national portal dedicated to offering support and reporting tools for revenge porn victims." READ MORE

Source: Europol

Date: 31 Oct 2017

Europol launches the SIRIUS platform to facilitate online investigations

"As criminals increasingly adopt the Crime-as-a-Service model, getting easy access to tools and services for digitally-enabled crimes, law enforcement authorities face a highly complex challenge when conducting criminal investigations online. To address this challenge, Europol officially launched the SIRIUS platform. SIRIUS is a secure web platform for law enforcement professionals, which allows them to share knowledge, best practices and expertise in the field of internet-facilitated crime investigations, with a special focus on counter-terrorism. […] The platform also addresses other challenges in criminal investigations, such as streamlining the requests to online service providers, and improving the quality of the responsive record." READ MORE

Source: The Hacker News

Date: 24 Oct 2017

Bad Rabbit: New Ransomware Attack Rapidly Spreading Across Europe

"A new widespread ransomware attack is spreading like wildfire around Europe and has already affected over 200 major organisations, primarily in Russia, Ukraine, Turkey and Germany, in the past few hours. Dubbed "Bad Rabbit," is reportedly a new Petya-like targeted ransomware attack against corporate networks, demanding 0.05 bitcoin (~ $285) as ransom from victims to unlock their systems. According to an initial analysis provided by the Kaspersky, the ransomware was distributed via drive-by download attacks, using fake Adobe Flash players installer to lure victims' in to install malware unwittingly." READ MORE

Source: Barbados Today

Date: 30 Oct 2017

Stronger laws coming to tackle cyber crime in Barbados

"Barbados' top judicial officer has warned about a growing class of sophisticated criminals in Barbados who is not only heavily armed but shoring up crimes with technology. Chief Justice Sir Marston Gibson today further cautioned that law enforcers and the judiciary had to keep one step ahead of criminals who were more organized and technologically savvy. […] Also addressing the workshop attended by top anti-crime officials, prosecutors and judicial officers, Attorney General Adriel Brathwaite said revisions were coming to the Computer Misuse Act, the Electronics Transfer Act, Telecommunications Act and the Copyright Act." READ MORE

Latest reports

- Council of Europe, Agenda of the 18th Cybercrime Convention Committee Plenary Meeting (T-CY) 27-29 November 2017, Version 31 Oct 2017
- European Commission, Tackling Illegal Content Online – Towards an enhanced responsibility of online platforms, 28 Sep 2017
- European Commission, First Annual Review of the EU-U.S. Privacy Shield, 18 Oct 2017
- European Union Agency for Fundamental Rights, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update, October 2017
- Europol, The Internet of Things: when your washing machine and blood pressure monitor become a target for cyberattacks, 19 Oct 2017
- ENISA, An overview of the Wi-Fi WPA2 vulnerability, 19 Oct 2017
- US-CERT, Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors, 23 Oct 2017
- Australian Security Intelligence Organisation, ASIO Annual Report 2016-17, October 2017

Upcoming events

- 28 October-3 November, Abu Dhabi, UAE – Participation in the ICANN60 Annual General Meeting, GLACY+
- 2-3 November, Bucharest, Romania – Regional workshop to assess the national regulatory framework for obtaining and using electronic evidence in criminal proceedings, iPROCEEDS
- 2-3 November, Chisinau, Moldova – Follow-up mission on various matters of public-private cooperation: Safeguards and operational agreements study visit, Cybercrime@EAP III
- 6-7 November, Tirana, Albania – Pilot introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors (2nd part), iPROCEEDS
- 6-7 November, Baku, Azerbaijan – Data preservation and retention workshop, Cybercrime@EAP III
- 6-9 November, Accra, Ghana – Advanced Judicial Course for judges, magistrates and prosecutors, GLACY+
- 6-9 November, Sarajevo, Bosnia and Herzegovina: Pilot training introductory training courses on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors, iPROCEEDS
- 6-10 November, Suva, Fiji – Participation of delegates from Tonga, Vanuatu and Samoa in the INTERPOL Cybercrime Training for the Pacific Region, GLACY+
- 9-10 November, Accra, Ghana – Advisory mission and workshop on Cybercrime Policies: Review of National Cybersecurity Policy & Strategy Document, GLACY+
- 13-14 November, Kyiv, Ukraine – Follow-up mission on various matters of public-private cooperation: Safeguards and operational agreements study visit, Cybercrime@EAP III
- 13-15 November, Dakar, Senegal – Advisory mission on the streamlining of procedures for mutual legal assistance related to cybercrime and electronic evidence, GLACY+
- 13-16 November, Pristina, Kosovo* – Case simulation exercises on cybercrime and financial investigations, iPROCEEDS
- 13-17 November, Tunis, Tunisia – Country assessment visit, CyberSouth

The Cybercrime Digest appears bi-weekly. News are selected by relevance to the current areas of interest to C-PROC and do not represent official positions of the Council of Europe. You receive this digest as you have taken part in Council of Europe activities on cybercrime. It is not intended for general publication.

For any additional information, contributions, subscriptions or removal from this distribution list, please contact: cybercrime@coe.int

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE