Cybercrime Digest

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

16-31 August 2016

Source: Ministère de l'Intérieur

Date: 23 Aug 2016

Initiative franco-allemande sur la sécurité intérieure en Europe

"Discours de Bernard Cazeneuve, ministre de l'Intérieur, lors de la conférence de presse commune avec Thomas de Maizière, ministre de l'Intérieur de la République Fédérale d'Allemagne, le 23 août 2016 à Paris: « […] Au niveau international, nous appelons à la signature et à la ratification de la Convention de Budapest sur la Cybercriminalité. En effet, la France estime que l'article 18 de cette Convention peut conférer une base légale à des réquisitions adressées par les autorités compétentes d'un pays partie à la convention en direction d'un fournisseur de services établi physiquement ou légalement à l'étranger, mais qui offre des prestations sur son territoire. »" READ MORE

RELATED ARTICLES

Initiative franco-allemande sur les enjeux clés de la coopération européenne dans le domaine de la sécurité intérieure, Ministère de l'Intérieur, 23 Aug 2016

Terrorisme: la France et l'Allemagne veulent encadrer les applications de messagerie, Le Figaro, 23 Aug 2016

Source: The Guardian

Date: 16 Aug 2016

Hacking group auctions 'cyber weapons' stolen from NSA

"A mysterious online group called the Shadow Brokers claims to have infiltrated an elite hacking unit linked to the National Security Agency and stolen state "cyber weapons", and is now auctioning them off to the highest bidder. The stolen malware is said to belong to Equation Group, a sophisticated hacking team believed to be operated by the NSA. So far, the Shadow Brokers have only released a few taster files and images of the cache, but security researchers said they appear to be legitimate. The leak, announced in broken English by the group in a series of posts on Twitter, Tumblr, Pastebin and Github, was accompanied by claims that the group was in possession of state-sponsored "cyber weapons". READ MORE

Source: Liberation

Date: 23 Aug 2016

Pédopornographie : le démantèlement d'un réseau européen conduit à 75 arrestations

"Les polices européennes ont arrêté 75 suspects dans 28 pays pour avoir partagé en ligne des images pédopornographiques, a indiqué Europol mardi dans le cadre d'une enquête sur plus de 200 dossiers. L'opération «Daylight» (lumière du jour, en français) a vu le jour après la réception d'informations venues de Suisse sur un vaste réseau de diffusion d'images d'abus sexuels sur des enfants, a affirmé à l'AFP la porte-parole d'Europol Claire Georges. «L'enquête a duré plus d'un an», a-t-elle ajouté, soulignant que des «dossiers d'informations», détaillant les suspects ou leurs adresses IP, avaient ensuite été envoyées à 26 pays à travers l'Europe, ainsi qu'en Norvège et en Suisse." READ MORE

Source : Lexology

Date : 24 Aug 2016

The New EU Cybersecurity Directive: What Impact on Digital Service Providers?

"On August 8, 2016, the Directive on Security of Network and Information Systems ("NIS Directive") entered into force … The NIS Directive provides guidelines for two types of entities: (i) "essential service operators" within the energy, transport, banking, financial market infrastructure, health, drinking water, and digital infrastructure sectors, and (ii) "digital service providers," including entities such as online marketplaces, online search engines, and cloud computing service providers. Considerable disagreement surrounded the inclusion of digital service providers within the draft NIS Directive …" READ MORE

Source: Gadget

Date: 24 Aug 2016

South Africa's new cybercrimes law explained

"A proposed new Cybercrimes and Cybersecurity Bill (Cybercrimes Bill) aims to stop cybercrime and to improve security for South African citizens. A draft of the Cybercrimes Bill was first released for public comment in August 2015, and submissions closed in December. The Bill is due to be presented to Parliament later this year." READ MORE

Source: DNA India

Date: 28 Aug 2016

Sri Lankan President Maithripala Sirisena's website hacked twice within two days

"Hackers tampered with Sri Lankan President Maithripala Sirisena's official website www.president.gov.lk on two consecutive days. The first attack occurred on Thursday evening, when hackers hijacked the site and posted a message in Sinhala, reports the Lanka Page. The message, posted under the name "The Sri Lankan Youth" […] also called on the government to be mindful about the security of Sri Lankan websites. Failure to do so could result in the country having to face a cyber war, the message warned." READ MORE

RELATED ARTICLES

Sri Lanka police arrest teen over hacking president's website, Reuters, 30 Aug 2016

Sri Lanka CERT takes steps to protect President Sirisena's official website from hackers, DBS Jeyaraj, 28 Aug 2016

Source: CPJ

Date: 24 Aug 2016

Proposed cyber-security bill threatens media freedom in Bangladesh

"The Committee to Protect Journalists called today on Bangladesh's legislature to scrap proposed cyber-security legislation that would impose severe penalties for disseminating online material deemed to be anti-state or a threat to national security or public order. The Digital Security Act 2016 was approved on August 22 by Prime Minister Sheikh Hasina's Cabinet and is pending in parliament, according to news reports. If passed into law, the bill will enable the creation of a new agency charged with monitoring for violations, including the use of electronic media to "carry out propaganda," "hurt religious sentiments," or "create enmity and disturb law and order," news reports said." READ MORE

Source: Journalism in the Americas

Date: 17 Aug 2016

Kenya: Hackers risk 20-year jail term in proposed law

"Hackers will face fines of up to Sh20 million and up to 20 years in jail under a new law aimed at taming cybercrime. Information, Communication and Technology Cabinet Secretary Joe Mucheru said security agencies would need training on how to handle crimes assisted by information technology while judicial officers would also need to upgrade their knowledge of such matters. Mucheru said the tough penalties are contained in the Computer and Cybercrime Bill, which is being prepared and is yet to be presented to the Cabinet for approval." READ MORE

Source: Journalism in the Americas

Date: 17 Aug 2016

St. Vincent and the Grenadines passes Cybercrime Bill that allows prison sentences for online defamation

"[…] Several provisions of this bill pose a serious threat to freedom of the press, the free flow of online information, and public debate," according to a joint statement from at least 25 freedom of expression organizations […]. The statement was released following the passage of the bill. The organizations pointed out that Grenada adopted a similar law in 2013, but then amended it because of international criticism. They also said that both Trinidad and Tobago and Guyana are looking at similar legislation." READ MORE

Source: International Business Times

Date: 16 Aug 2016

Australian authorities hacked computers in the US while investigating dark web child abuse site

"Tor users in the US were allegedly hacked by Australian authorities, as part of a child pornography investigation, which involved a prolific dark web child abuse site called "The Love Zone". The law-enforcement led-hacking came to light, thanks to court documents recently filed in the US. […] The task force then posed as the site's owner in an undercover operation to go after the site's members." READ MORE

Source: The New Times

Date: 28 Aug 2016

INTERPOL partners Rwanda for training on cyber-enabled crimes

"Enhancing the ability of law enforcement to investigate cyber-enabled human trafficking is the focus of a regional table-top exercise organized by the Rwanda National Police (RNP) and INTERPOL. Gathering some 90 participants from more than 30 countries, the five-day (29 August – 2 September) […] Participants at the table-top exercise will use criminal investigation methodology and skills learned in training to address the practical challenges necessary to undertake cybercrime investigations." READ MORE

Source: VOA

Date: 25 Aug 2016

Social media crackdown: the new normal for Africa?

"Police in Burundi arrested eight people Saturday for allegedly circulating defamatory anti-government statements on social media. The Burundi case is not unique. The list of African countries trying to cut or control social media keeps growing, particularly during elections or periods of unrest." READ MORE

Source: Security Week

Date: 25 Aug 2016

25 Million Accounts stolen from mail.ru domains

"LeakedSource, a service that allows users to check if their online accounts have been compromised, reported on Wednesday that cybercriminals obtained roughly 25 million username and password combinations from three different domains: cifre.mail.ru, parapa.mail.ru and tanks.mail.ru. The affected domains host forums for games acquired by the Mail.Ru Group over the past years." READ MORE

Source: The Hacker News

Date: 24 Aug 2016

ATMs in Thailand Hacked; 12 Million Baht Stolen; 10,000 ATMs Prone to Hackers

"An Eastern European gang of criminals has stolen over 12 Million Baht (approximately US$350,000) from a total of 21 ATMs in Bangkok and other five provinces by hacking a Thai bank's ATM network; police said Wednesday. The Central Bank of Thailand (BoT) has issued a warning to all commercial banks about security flaws in roughly 10,000 ATMs, exploited to steal cash." READ MORE

Latest reports

- Council of Europe, Draft Outline of the Octopus Conference on 16-18 November 2016 in Strasbourg, Version June 2016
- ASSOCHAM-PwC, India registers 350% rise in cybercrime in three years, 25 Aug 2016
- FireEye, M-TRENDS 2016 - Asia Pacific edition, August 2016
- PaloAlto, Exploring the Cybercrime Underground, Part I, Part II, 19 Aug 2016, 29 Aug 2016

Upcoming events

- 5 – 7 September, Kyiv, Ukraine - Workshop on procedural powers of the law enforcement and security agencies, including execution of requests received via 24/7, EAP II
- 6 – 9 September, Johannesburg, South Africa – Progress review meetings and updated situation reports, GLACY/ GLACY+
- 7 – 8 September, Belgrade, Serbia – Advisory mission and workshop for the setting up or improvement of reporting mechanisms, iPROCEEDS
- 8 – 9 September, Kyiv, Ukraine – Amendments to procedural law: assessment visit, EAP III
- 13 – 15 September, Finland – Regional Internet Security Event (RISE), iPROCEEDS
- 15 – 16 September, Minsk, Belarus - Workshop on development of legal instruments on cybercrime and amendments to existing legislation, EAP II

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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime