Cybercrime Digest

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

1-15 September 2016

Source: Council of Europe

Date: 15 September

Octopus Conference 2016

Registration for the Octopus Conference on Cooperation against Cybercrime is now open. The event will take place at the Council of Europe in Strasbourg from 16 to 18 November 2016. It will focus on criminal justice access to electronic evidence in the cloud and on the 15th anniversary of the Budapest Convention on Cybercrime. READ MORE

Source: Ars Technica

Date: 2 Sep 2016

Microsoft, Salesforce, Google all sign up for EU-US Privacy Shield

"[…] Privacy Shield is a voluntary scheme, whereby companies promise to treat European citizens' personal data in compliance with European Union data rules. Those pledges are then enforced by the US department of commerce. According to the commission, the department of commerce is currently reviewing the privacy policies of 190 further firms that want to sign up, while an additional 250 companies are in the process of submitting their applications." READ MORE

Source: Le Point

Date: 13 Sep 2016

La France a subi une vingtaine de cyberattaques majeures en 2015

"Une vingtaine de cyberattaques majeures ont ciblé en 2015 les intérêts français, révèle l'Agence nationale de la sécurité des systèmes d'information (Anssi) dans son premier rapport annuel, publié mardi 13 septembre. Les noms des cibles, "avant tout privées", ne peuvent toutefois pas être dévoilés : des géants du CAC40 pourraient y perdre la tête. Au total, plus de 2 300 codes malveillants ont été collectés et 4 000 signalements ont été reçus par l'agence de cyberdéfense en 2015, soit 50 % de plus qu'en 2014. La motivation des attaquants est, le plus souvent, l'espionnage économique : essayer de voler des informations sur les clients, sur les réponses aux appels d'offres ou encore sur les savoir-faire." READ MORE

Source: Cameroun-Info.net

Date: 7 Sep 2016

Cameroun – La cyber criminalité fait perdre 4 milliards de FCFA au Trésor public camerounais

"Les chiffres rendus publics par l'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC) révèlent qu'en 2015 le trésor public camerounais a enregistré des pertes financières d'un peu plus de 4 milliards de FCFA du fait de la cyber criminalité. Toujours dans la même année, quatre opérateurs de téléphonie mobile présents au Cameroun ont eu des pertes financières chiffrées à 18 milliards de FCFA." READ MORE

Source: Bangladesh News

Date: 2 Sep 2016

Philippine justice department finishes probe on $15m of $81m Bangladesh Bank heist

"The pending cases at the DOJ cover $15 million of the $81 million funds stolen in February in the world's largest known cyber bank heist. Aside from that, the Philippine Amusement and Gaming Corp has managed to recover $2.7 million until now. Total $63 million more of the stolen money remain missing. Bangladeshi officials are still pursuing that. […] The stolen funds then ended up in casinos which are not covered by the anti-money laundering law." READ MORE

Source: Net Politics

Date: 2 Sep 2016

Brazil Must Rebalance Its Approach to Cybersecurity

"[…]Brazil could also consider joining the other 49 countries that have signed and ratified the Budapest Convention, a framework that facilitates international cooperation on fighting cybercrime while protecting human rights and due process. While Brazil has complained about not being involved in its original drafting, it is the only internationally-binding instrument to address cybercrime. At a minimum, the government needs to require greater transparency of service providers and financial institutions to ensure a more data-driven approach to cybersecurity." READ MORE

Source: Leaked Source

Date: 6 Sep 2016

98.1 Million accounts stolen from Russian web portal Rambler

"Another day, another mega breach. Today, LeakedSource announced that almost 100 million, or 98,167,935 to be exact, accounts for the popular Russian portal Rambler.ru were leaked online. What makes this worse was that Rambler was storing account passwords in plain text rather than being encrypted. This means that anyone who was able to hack their database had full access to the user's passwords without having to crack them first." READ MORE

Source: Data Breach Today

Date: 1 Sep 2016

State Governments' war against cybercrime in India

"Following cyberattacks on public and private organizations, state governments in India are rolling up their sleeves to fight cybercrime. For example, Maharashtra Chief Minister Devendra Fadnavis announced the "Maharashtra Cyber Project" on Independence Day, planning 51 cyber labs across districts providing technical and forensic investigation support to the cyber police. The project also will launch a computer emergency response team, or CERT. Three other states - UP, Karnataka and Kerala states - that have already set up cyber labs intend to scale up and emulate the Maharashtra model." READ MORE

Source: Anadolu Agency

Date: 31 Aug 2016

Rwanda says Africa must prioritize fighting cybercrime

"Rwanda's president backed a $1.5-million cybercrime project with Interpol on Wednesday, telling African police forces to work together on the growing threat. President Paul Kagame addressed a gathering of close to 100 African police heads during a cybersecurity exercise organized by Interpol and hosted in the Rwandan capital, Kigali." READ MORE

Source: Reuters

Date: 1 Sep 2016

Romanian hacker 'Guccifer' sentenced to 52 months in U.S. prison

"A Romanian hacker nicknamed "Guccifer" who helped expose the existence of a private email domain Hillary Clinton used when she was U.S. secretary of state was sentenced on Thursday to 52 months in prison by a federal court in Alexandria, Virginia. Marcel Lazar, 44, who used the alias online, had pleaded guilty in May to charges including unauthorized access to a protected computer and aggravated identity theft after being extradited from Romania." READ MORE

Source: Security Affairs

Date: 4 Sep 2016

Dutch Police seize two servers of the Switzerland-based VPN provider Perfect Privacy

"Recently the Dutch Police has seized two servers belonging to Switzerland-based Virtual Private Network (VPN) provider Perfect Privacy, as part of an investigation. At the time I was writing the Dutch police hasn't provided further details about the seizures. The Perfect Privacy VPN provider informed its customers that two servers in Rotterdam were seized by the Dutch police on Thursday, August 24. The Dutch authorities seized the servers of the company, they requested the I3D to give them the access to the servers with a subpoena that allowed them to seize the hardware." READ MORE

Source: Government of Republic of Mauritius

Date: 31 Aug 2016

SADC Workshop shares best practices on Cybersecurity in Mauritius

"A SADC Workshop on Cybersecurity and PKI (public key infrastructure), aiming at sharing best practices and strengthening SADC regional cooperation mechanisms pertaining to cybercrime offenses and developing a Framework for PKIs for SADC Member States, opened yesterday at the Intercontinental Hotel, Balaclava. Organised by the Ministry of Technology, Communication and Innovation in collaboration with the Southern African Development Community, the four-day event is bringing together more than 50 participants coming from countries in the African region namely: Lesotho, Malawi, Mozambique, Mauritius, Seychelles, South Africa, Swaziland, Tanzania, Zambia and Zimbabwe." READ MORE

Source: Radio NZ

Date: 15 Sep 2016

Papua New Guinea cyber-crime laws dampen public discussion

"Papua New Guinea's new cyber-crime laws are already having a dampening effect on social media in the country. This is according to the founder of one of the first public Facebook groups "PNG Sharptalk" which has just over 26,400 active members. On 11th August PNG's parliament passed the Cybercrime Bill, aiming to control activities like spam, hacking, forgery and computer fraud. Douveri Henao supports having rules and guidelines for social media engagement, but he says since the legislation was passed there has been a noticeable change in the way people engage online. Mr Henao said this is particularly true for social media pages which previously gave free rein to members voicing their frustrations." READ MORE

Source: The Borneo Post

Date: 3 Sep 2016

Malaysian Communications Multimedia Commission lauds establishment of special cyber court

"The Malaysian Communications and Multimedia Commission lauds the setting up of the special court for cyber crimes, saying it is timely. The cyber court began operating a few days ago at the court complex in Jalan Duta, Kuala Lumpur. "Hopefully, cyber cases that had been investigated by MCMC under the Communications and Multimedia Act 1998, particularly social media misuse would be dealt with by the court expeditiously," it said." READ MORE

Source: Standard Media

Date: 14 Sep 2016

Why companies in Kenya should tame cyber crime

"It is estimated that 70 per cent of Kenyan businesses are vulnerable to cybercrime and the country loses about Sh15 billion annually due to the crime. Part of the reason for the growing prevalence of cybercrime in Kenya is the country's increasing digitization, which has inadvertently exposed Kenyans to cybercriminals. Furthermore, key stakeholders don't fully appreciate the full range of risks that they are exposed to or how to mitigate against them." READ MORE

Source: Balancing Act

Date: 13 Sep 2016

Zambia set to pass cybercrime law

"An Internet crime bill in Zambia, which includes provisions that could see convicted hackers facing sentences of up to 25 years in jail, has caused some controversy in the country's IT community but is expected to become law soon. The bill received parliamentary approval and is expected to be signed into law by President Levy Mwanawasa within a month or two. The bill would become the first Zambian law dealing with cybercrime. Minister of Transport and Communications Bates Namuyamba introduced the bill in Parliament last month, following the government's completion of its Information and Communications Technology policy." READ MORE

Source: Electronic Frontier Foundation

Date: 9 Sep 2016

Cybercrime Law and freedom of speech in Arab Countries

"In reaction to fundamentalist groups often relying on the Internet for propaganda and recruiting, several governments in the Arab world have passed shortsighted cybercrime and counterterrorism laws – ostensibly to combat these groups on the digital front. [Such laws] explicitly criminalize speech that the government finds threatening to its legitimacy, and are often used to supplement other totalitarian practices to target and stifle unwanted or politically critical speech." READ MORE

Latest reports

- European Parliament – LIBE Committee, Cyberbullying among young people, July 2016
- ENISA, Annual Report 2015, 9 September 2016
- ANSSI, Premier Rapport Annuel 2015, 13 September 2016
- UK National Audit Office, Protecting information across government, 14 September 2016
- Nokia, Threat Intelligence Report 1H2016, 1 September 2016

Upcoming events

- 15 – 16 September 2016, Minsk, Belarus – Workshop on development of legal instruments on cybercrime and amendments to existing legislation, EAP II
- 19 – 20 September 2016, Minsk, Belarus – Second Regional meeting on LEA/ISP Cooperation Platform, EAP III
- 19-22 September 2016, Santo Domingo, Dominican Republic - Initial Assessment mission, GLACY+
- 23-25 September 2016, Colombo, Sri Lanka – Support to national delivery of introductory judicial course, GLACY
- 28 – 30 September 2016, Singapore – 4th INTERPOL-Europol Cybercrime Conference "Solutions for attribution", EAP II, GLACY+, iPROCEEDS
- 28-30 September 2016, New Delhi, India – Participation in CyFy: The India Conference on Cyber Security and Internet Governance, Octopus project
- 29 – 30 September 2016, Tirana, Albania – Advisory mission and workshop for the setting up or improvement of reporting mechanisms, iPROCEEDS
- 29-30 September 2016, Lima, Peru - Introductory training course on cybercrime and electronic evidence for judges and prosecutors in Peru, Octopus project

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