Cybercrime Digest

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

1-15 January 2017

Source: European Commission

Date: 10 Jan 2017

European Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions

"The Commission is proposing new legislation to ensure stronger privacy in electronic communications, while opening up new business opportunities. The measures presented today aim to update current rules, extending their scope to all electronic communication providers. They also aim to create new possibilities to process communication data and reinforce trust and security in the Digital Single Market – a key objective of the Digital Single Market strategy. At the same time, the proposal aligns the rules for electronic communications with the new world-class standards of the EU's General Data Protection Regulation. The Commission is also proposing new rules to ensure that when personal data are handled by EU institutions and bodies privacy is protected in the same way as it is in Member States under the General Data Protection Regulation, as well as setting out a strategic approach to the issues concerning international transfers of personal data." READ MORE

RELATED ARTICLES

European Commission, Proposal for a Regulation on Privacy and Electronic Communications, 10 January 2017

Source: The World Post

Date: 9 Jan 2017

German Government Closely Watching Reports Of Russian Fake News Campaign

"German government officials on Monday said they were carefully examining an unprecedented proliferation of fake news items amid intelligence agency reports of Russian efforts to influence the country's parliamentary election in September. The BfV domestic intelligence agency also confirmed that a December cyber attack against the OSCE used the same tools seen in a 2015 hack of the German parliament that was attributed to the APT28 Russian hacking group. Russia denies being involved in any cyber warfare targeting Western governments and institutions." READ MORE

Source: Security Week

Date: 11 Jan 2017

Italian Siblings Arrested Over Long-running Cyber Espionage Campaign

"Italian siblings Giulio Occhionero and Francesca Maria Occhionero have been arrested in Rome, charged with conducting a long-running cyber espionage campaign against leading Italian politicians, businessmen and Masons. The malware supposedly used by the duo is known as EyePyramid, possibly referencing the Eye of Providence found on the US one-dollar bill and often associated with Freemasonry. Investigators believe that the operation may have been running as early as 2010." READ MORE

RELATED ARTICLES

Kaspersky GReAT, The "EyePyramid" attacks, 12 January 2017

Source: The Guardian

Date: 5 Jan 2017

Children in England sign over digital rights 'regularly and unknowingly'

"Almost half of eight- to 11-year-olds have agreed impenetrable terms and conditions to give social media giants such as Facebook and Instagram control over their data, without any accountability, according to the commissioner's Growing Up Digital taskforce. The year-long study found children regularly signed up to terms including waiving privacy rights and allowing the content they posted to be sold around the world, without reading or understanding their implications. Children's commissioner Anne Longfield said children needed a specialist ombudsman to represent their rights to social media companies and recommended a broader digital citizenship programme should be obligatory in every school from ages four to 14." READ MORE

Source: Le JDD

Date: 8 Jan 2017

Le Ministre de la Défense: "Face à une cyberattaque, la France peut riposter par tous les moyens"

"Jean-Yves Le Drian, ministre de la Défense, détaille au JDD, les moyens mis en oeuvre par le gouvernement pour lutter contre les cybermenaces alors que les autorités américaines accusent la Russie de piratage informatique contre le parti démocrate pendant la campagne présidentielle." READ MORE

Source: African Business Review

Date: 9 Jan 2017

Collaboration is vital to Africa's cyber-security tactics

"The most serious issue is the significant gap between the scale of Africa's cyber-security capability and the increased availability of internet-enabled devices to a wider cross-section of the population. Cyber-crime affects ordinary citizens in Africa – it is estimated that Kenyans lost $23,000,000 last year as a result of fraud – and costs the economy millions. It's impossible to calculate the damage done to Nigerian businesses, which have been virtually blacklisted by retailers around the world as they increasingly refuse to ship to a country that has become a by-word for online scams in recent years." READ MORE

Source: Motherboard

Date: 7 Jan 2017

As Afghanistan Comes Online, It Grapples With Its First Cyber Security Laws

"[…] The Afghan Cyber Security Bill, prepared by the Afghan Ministry of Communication, Information and Technology (MCIT), lays down definitions of cybercrime and procedures to tackle them within the purview of the existing criminal law. The law also proposes that there needs to be a separate court to deliberate on cybercrimes, asks for an office under the Attorney General for matters of cyber offences, and someone trained specifically to handle these cases. At face value, the law is rather impressive, borrowing from and adopting best practices from around the world. But a detailed peek into the document reveals an overtly ambitious plan, the implementation of which would require logistical and procedural systems that do not yet exist in Afghanistan." READ MORE

Source: Zimbabwe Independent

Zimbabwe Cybercrimes Bill: Its flaws, remedies

"The Zimbabwe chapter of the Media Institute of Southern Africa (Misa-Zimbabwe), working with the Digital Society of Zimbabwe, has come up with a position paper on

Date: 13 Jan 2017

the Computer Crime and Cybercrime Bill, which was introduced last year by government to curb cybercrime. […] Misa states that the Bill, which has been amended several times now, infringes on basic people's rights, including freedom of expression. Misa is advocating for wider consultation before the Bill can be brought to parliament for debate so that the content reflects the will of the people and not the machination of a political party to maintain its grip on power. The position paper, which was formulated in November, will form part of civil society's talking points in coming up with a model Cybercrime law to be presented to government for debate." READ MORE

Source: Associated Press

Date: 7 Jan 2017

Baltic news agency targeted by cyber attack

"A cyber attack disrupted services for 10 hours at the main Baltic news agency in Estonia, bosses said on Saturday. The Tallinn-based Baltic News Service said the attackers targeted "servers in the BNS network" at around 2pm on Friday. The agency said it managed to get the system up and running again around midnight on Friday, adding that its services were functioning normally on Saturday. BNS did not say who it suspected was behind the attack." READ MORE

Source: GMA News

Date: 9 Jan 2017

Hackers hit journalists' website in the Philippines

"The website of the National Union of Journalists of the Philippines (NUJP) was hacked on Monday evening and could not be accessed. NUJP Chairman Ryan Rosauro told GMA News Online the site was down by 8 p.m. and cannot be accessed even by the website's administrator. He also said this is the first time the group's website was hacked." READ MORE

Source: Nyoooz

Date: 13 Jan 2017

Cyber offences keep rising in India, lack of training hurts probe

"Prosecutors should be given training so that they understand technical details of the cases, said the experts. "The government should bring in private agencies who can train the cyber police on methods to collect evidence and guard against tampering." A dedicated metropolitan court for trying cybercrime matters, more staff in cyber forensics lab, and more cyber police stations, all on one premise, will also help get convictions." READ MORE

Source: Daily News

Date: 9 Jan 2017

Tanzania, fight against cybercrime is here to stay

"The recent High Court's decision confirmed the Cybercrimes Act does not abrogate the Constitution of the United Republic of Tanzania. A bill for such law was moved by the Attorney General, the government's chief legal advisor before the National Assembly in April 2015 where it was widely discussed before being endorsed and later accorded presidential assent to become a law of the land. The objectives of Cybercrimes Act No. 14 of 2015 include, among others, to provide a framework for the protection of individual rights and freedoms against cybercrimes and provide mechanism and framework of combating cybercrimes. Also to establish offences and punishments relating to cybercrimes and to outline rules and procedures for the investigation and prosecutions, to provide for rules on the liability of service providers in relation to crimes and to provide protection of the national economy, financial services against cybercrimes." READ MORE

Source: Latin America Herald Tribune

Date: 13 Jan 2017

Human Rights Watch Slams Internet Censorship Laws in Southeast Asia

"Southeast Asian governments are trying to curb freedom of expression on the internet through laws aimed at suppressing criticism by citizens and independent organizations, Human Rights Watch said Friday. HRW Asia deputy director Phil Robertson told EFE that governments in the region are increasingly putting in jeopardy people's rights to say what they want online and to form groups to stand up for their rights. Saying governments in the region perceive the internet as a threat, he added that several new cyber-crime laws are directed at keeping people compliant so that governing elites can continue to reap the social and economic benefits of the status quo." READ MORE

Source: Gulf News Journal

Date: 9 Jan 2017

Saudi Arabia wrestles with cybercrime in social media era

"In Saudi Arabia, the full spectrum of issues surrounding cybercrime tangles with traditional attitudes about moral values to create quite a complex navigational field for social media users. A December 2016 opinion piece by a private party, Saeed Al Qahtani of the corporate law firm Al Tamimi and Company, discussed the Saudi Anti-Cyber Crime Law, which protects the rights of users and the integrity of the internet, along with safeguards for data, an effort to protect public morality, and individual privacy. One of the things the Qahtani wrestled with is the effort to distinguish between deliberate and willful cybercrime acts and everyday content social media users might transmit without knowing they're involved in criminal activity." READ MORE

Source: Deep Dot Web

Date: 7 Jan 2017

Darknet Drug Purchases Increase by 2.2%

"Two major global drug studies from Global Drug Survey and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) emphasized the impact of the darknet on the rising global drug usages. EMCDDA specifically noted the rise of cryptomarkets such as AlphaBay that accept anonymous cryptocurrencies including Monero to facilitate transactions. […] Tightening Know Your Customer (KYC) and Anti Money Laundering (AML) policies on bitcoin exchanges and service providers have made bitcoin even more accessible by law enforcement, as it allows local authorities to demand personal information and financial data from trading platforms. With that, agencies can track down a bitcoin transaction, find its correlation with an exchange, unravel user information and ultimately, crackdown the illicit drug buyer." READ MORE

Source: Softpedia

Date: 14 Jan 2017

Government of Venezuela Websites Hacked

"Three websites operated by Venezuela's government were hacked recently by Kapustkiy, who managed to access private databases containing sensitive information. The three sites are snv.gob.ve, estudiosydesatres.gob.ve, and sunaval.gob.ve, all of which belong to different departments of the Venezuelan government and which allegedly contained vulnerabilities that were exploited by white hacker Kapustkiy. In a statement provided to Softpedia earlier today, Kapustkiy says the cyberattack was launched in protest against the dictatorship of president Nicolas Maduro - this is the second time he hacks websites belonging to the Venezuelan government with this particular idea in mind." READ MORE

Source: Graphic Online

Date: 14 Jan 2017

Fight against cybercrime in Ghana

"The fight against cyber crime requires high technological-savviness and multiple dimensions, the Director of the Cyber Crime Unit of the Criminal Investigations Department (CID) of the Police Service, Chief Superintendent of Police Dr Herbert Gustave Yankson, has said. He explained that cyber crime was multi-faceted and sophisticated and, therefore, required a collective responsibility to deal with. […] "We all have a role to play. It is not all about the police, but it is about all service providers, the academia, journalists and policymakers," he said." READ MORE

Latest reports

- CSIS Cyber Policy Task Force, From awareness to action – a cybersecurity agenda for the 45th President, January 2017
- ENISA, Cyber Security and Resilience of smart cars, 13 January 2017
- IGF, Summary Report: Internet Governance Forum 2016, 8 January 2017
- NIST, Framework for Improving Critical Infrastructure Cybersecurity – Draft Version 1.1, 10 January 2017
- CLUSIF, Panorama de la cybercriminalité, Janvier 2017
- Front Line Defenders, Annual Report on Human Rights Defenders at Risk in 2016, 1 January 2017
- Forbes, The Top Cyber Security Risks In Asia-Pacific In 2017, 11 January 2017
- Techweez, Kenya ICT Law in 2016 - Year Review, 6 January 2017

Upcoming events

- 16 – 17 January 2017, Belgrade, Serbia – Workshop on online financial fraud and credit card fraud, iPROCEEDS;
- 16 – 17 January 2017, Senegal – Advisory mission and workshop on Cybercrime Policies, GLACY+;
- 10 – 20 January 2017, Ghana – Advisory mission and workshop on Cybercrime Policies GLACY+;
- 23 – 25 January 2017, Georgia - Development of the Cyber Exercise scenarios with Data Exchange Agency, EAP III;
- 25 – 26 January 2017, Nairobi, Kenya – Participation of 5 African LEA representatives from Ghana, Senegal, Morocco and Mauritius in the ICANN Capacity building workshop, GLACY+;
- 26 – 27 January 2017, Mauritius and Philippines – Study visit of the Philippines delegation to Mauritius CERT, GLACY+.

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