Cybercrime Digest

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

16-31 January 2017

Source: Presidency of Romania

Date: 24 Jan 2017

Joint press conference by Mr. Klaus Iohannis, the President of Romania, and Mr. Thorbjørn Jagland, the Secretary General of the Council of Europe

"[…] We have discussed about many important topics, especially how to increase our concrete cooperation. Romania is a staunch supporter of the values of the Council of Europe, especially those related to the rule of law, which are sometimes challenged in some of the member states. […] We also talked about the activity of the Cybercrime Programme Office of the Council of Europe in Bucharest, which is perhaps the best result oriented Office of the Organization, with a range of concrete projects reaching beyond the geographic area of the Council." READ MORE

Source: Council of Europe

Date: 24 Jan 2017

Greece ratifies the Budapest Convention and its Protocol on Xenophobia and Racism

"Today, Greece deposited the instrument of ratification and became the 52 State Party to the Budapest Convention on Cybercrime. Another 15 have either signed or been invited to accede. Greece also deposited the instrument of ratification to the Protocol on Xenophobia and Racism. 27 States are now Party to the Protocol." READ MORE

Source: Der Spiegel

Date: 18 Jan 2017

Fake News: The Secretary General of the Council of Europe warns against censorship

"The Secretary General of the Council of Europe has cautioned governments over state measures to combat fake news. "We should be careful with content which is not evidently illegal" said Thorbjørn Jagland to German Press Agency dpa. "This can lead to a kind of censorship and be used in the wrong way." […] Jagland also raised the issue of Internet hacking, saying "this is the greatest threat". The Council of Europe is currently updating the Cybercrime Convention to allow security services to access data stored on servers [and in the Cloud]. The President of Germany's Constitutional Protection Agency, Hans-Georg Maaßen, recently made similar proposals following concerns over hacking during the US election campaign and ahead of parliamentary elections in Germany." READ MORE (German) / English version

Source: Irish Legal News

Date: 26 Jan 2017

Bill to meet EU cybercrime obligations passes second stage in Ireland

"Legislation to incorporate EU rules on cybercrime into Irish law has been approved by TDs at the second stage in the Dáil. Commending the Criminal Justice (Offences Relating to Information Systems) Bill to TDs, minister of state David Stanton said the reforms were essential. The main purpose of the bill is to give effect to provisions of EU Directive 2013/40/EU on attacks against information systems. It will also give effect to many of the key provisions of the Budapest Convention on Cybercrime, which Ireland signed in 2002." READ MORE

Source: Daily Mail

Date: 24 Jan 2017

Europe's security chief warns of growing threat of cyber attacks by criminals and the EU's political enemies

"The EU's security chief has warned Europe faces a 'growing threat' of cyber attacks by criminals and the organisation's political enemies. EU security commissioner Julian King said Brussels must shore up its defences in the face of a mounting danger. He gave the example of the European Commission, the EU's powerful executive, which was hit by a 20-percent surge in cyber-attacks last year. Speaking ahead of a cyber security conference in Lille, he said cybercrime cost the European economy 'nearly 60billion euros in 2016' and the bill will continue to rise." READ MORE

Source: Europol

Date: 27 Jan 2017

Members of an international cybercrime syndicate active in Europe and Asia apprehended

"Five members of an international organised criminal group (OCG) have been arrested and three of them convicted so far as a result of a complex operation led by law enforcement agencies from Europe and Asia, with the active support of Europol's European Cybercrime Centre (EC3). This organised crime group is responsible for carrying out highly-sophisticated attacks against banks' ATMs which were made to dispense all the money deposited inside. One arrest has been made by the Romanian National Police, three arrests by the Taiwanese Criminal Investigation Bureau and one arrest by the Belarusian Central Office of the Investigative Committee." READ MORE

Source: CNBC

Date: 24 Jan 2017

UK fraud hits record high after increase in cyber attacks

"The value of alleged fraud cases reaching U.K. courts totalled more than £1.1 billion ($1.36 billion) in 2016 as the increasing risk of cyber-attacks and large-scale scams continue to threaten businesses, according to a report from accountancy giant KPMG. A 55 percent year-on-year rise in the value of fraud from the previous year was largely due to a resurgence in so-called super cases, or incidents worth over £50 million. Though the cost of fraud in the U.K. was much higher than in previous years, the number of incidents was lower." READ MORE

Source: All Africa

Date: 19 Jan 2017

South Africa's Cyber Crimes and Cyber Security Bill to be introduced to the Parliament in the next few weeks

"Statement by the Deputy Minister of Justice and Constitutional Development, the Hon JH Jeffery, MP. «[…] Deterring cybercrime is a vital component of a national cybersecurity and critical information infrastructure protection strategy. This includes the adoption of appropriate legislation against the misuse of information communications technologies for criminal purposes. The new Bill aims to advance these objectives. […] The Bill contains a number of new criminal offences. The conduct which the Bill aims to criminalise is substantially in line with cybercrime legislation of various countries, the African Union Convention on Cyber Security and Personal Data Protection, the Budapest Convention on Cybercrime and various model laws […]. The Bill will be introduced in the next few weeks into Parliament»." READ MORE

Source: Observatoire-FIC

Date: 09 Jan 2017

La lutte contre la Cybercriminalité au Maroc, les réalisations et quelques défis

"[…] Menacé par le phénomène de la cybercriminalité, le Maroc est aussi conscient de cette dualité entre la nécessité de la transformation numérique et le risque cybernétique, par conséquent depuis une décennie le Maroc a mis en place une stratégie nationale de cybersécurité et de sécurité des systèmes d'information favorisant la transformation vers l'économie numérique et vers la société de l'Information et de la communication […]. Sur le plan réglementaire, le Maroc a mis à jour ses textes de lois surtout le code pénal et a mis en place de nouveaux décrets et lois relatives à la réglementation numérique telle le cas de la loi 53- 05 relative à l'échange électronique de données juridiques, la loi 09-08 relative au traitement automatisé des données personnelles, sans oublier la ratification de conventions internationales en matière de lutte contre la cybercriminalité et le terrorisme via les moyennes technologique de communication, à savoir par exemple la Convention de Budapest relative à la cybercriminalité […]." READ MORE

Source: GhanaWeb

Date: 25 Jan 2017

Ghana advances its national policy on cyber security

"[…] The policy, which was approved by cabinet in 2016, is a road map on what should be done to ensure that the country's cyberspace is secure. The policy also talks about issues within the cybercrime law enforcement area which currently is difficult for the law enforcement to implement because of the lack of capacity and necessary tools. It has, therefore, outlined areas such as building the capacities of law enforcement bodies, as well as the legal fraternity such as the Attorney-General, judges and lawyers to empower them to deal with cybercrime-related issues." Council of Europe advised on possible ways forward for making the strategy fully compliant with international standards substantiated in the dispositions of the Budapest Convention." READ MORE

RELATED ARTICLES

Council of Europe, GLACY+: Ghana advances its national cybersecurity strategy, 20 Jan 2017

Graphic Online, NITA develops cybercrime alert portal, 28 Jan 2017

Source: Rappler

Date: 27 Jan 2017

Online libel tops cybercrime cases in the Philippines for 2016

"From 2013 to 2015, online scams consistently topped the list of most common cybercrimes reported to the Philippine National Police-Anti-Cybercrime Group (PNP-ACG). But in 2016 – a year of heated political debates that also took place in cyberspace – online libel emerged as the top complaint of Filipino internet users, with 494 complaints recorded compared to 311 recorded in 2015. It comprised 26.49% of the 1,865 cybercrime complaints for 2016. Meanwhile, online scam complaints came in at second place, with 444 complaints in 2016, up from the 334 complaints recorded in 2015. Rounding up the top 5 complaints were identity theft, online threats, and violation of the anti-photo and video voyeurism act." READ MORE

RELATED ARTICLES

BusinessMirror, Cyberlibel, 29 Jan 2017

Source: Naked Security

Date: 25 Jan 2017

Court rejects US government appeal in case of Microsoft overseas email

"A US appeals court won't revisit its decision to deny Department of Justice efforts to make Microsoft turn over customer emails stored overseas. According to Grant Gross of the IDG News Service, the US Court of Appeals for the Second Circuit ruled in a 4-4 decision that it will not reverse its July decision to deny DOJ access to the email of a drug trafficking suspect stored on a Microsoft server in Ireland. Microsoft has fought the DOJ requests for more than three years." READ MORE

Source: ThreatPost

Date: 23 Jan 2017

Massive Twitter Botnet Dormant Since 2013

"A sizable and dormant Twitter botnet has been uncovered by two researchers from the University College London, who expressed concern about the possible risks should the botmaster decide to waken the accounts under his control. Research student Juan Echeverria Guzman and his supervisor and senior lecturer at the college Shi Zhou told Threatpost that the 350,000 bots in the Star Wars botnet could be used to spread spam or malicious links, and also, more in line with today's social media climate, start phony trending topics, attempt to influence public opinion, or start campaigns that purport a false sense of agreement among Twitter users." READ MORE

Source: Daily Sabah

Date: 25 Jan 2017

Experts draw attention to Turkey's need of cybersecurity for national security

"Ankara-based think tank, the Foundation for Political, Economic and Social Research (SETA), organized a panel yesterday in which experts called for an immediate cybersecurity strategy to combat cyber-threats against Turkey's national security and border security. While experts expect increased cyberattacks against Turkish authorities in 2017, they drew attention to the need to raise awareness of the cybersecurity issue and create human resources by educating engineers in this field. Regarding Turkey's capacity in cybersecurity, SETA Security Researcher Merve Seren, emphasized that the crucial point is to produce secure software programs to protect information concerning weapon systems, battleships and cryptography." READ MORE

Source: TechWeez

Date: 23 Jan 2017

African Countries in Capacity Building Efforts to Harness Internet Opportunities

"African countries have intensified efforts to build relevant capacity on the continent to fully exploit opportunities presented by the internet. With the internet permeating virtually every aspect of life, in Africa, businesses and governments are increasingly relying on internet as a vehicle for transformation. However, insufficient skills have slowed down the continent's utilization of the internet's benefits. Deliberate steps are necessary to address the capacity challenges. Delegates from the region and officials from the global body responsible for assigning names and numbers, converged in Nairobi today to discuss how to leverage on the positive impact of the internet and how it can be translated into meaningful socio-economic gains." Council of Europe contributed to the workshop, presenting its capacity building initiatives on cybercrime and electronic evidence, currently being developed in the African region." READ MORE

Source: Al Monitor

Date: 29 Jan 2017

How Palestinian authorities plan to clamp down on cybercrime

"On Jan. 2, Palestinian Authority (PA) Attorney General Ahmed Barak issued a decision to commission members of the Public Prosecution to start operating the Cybercrime Task Force in preparation for the issuance of the Cybercrime Law, which is expected to be passed in the first quarter of the year. The establishment of a cybercrime task force in Palestine aims to deter e-crimes, which many Palestinians are falling victim to and are not reporting to the police out of fear and intimidation. The law would address all forms of electronic crimes, in light of the recent high number of cybercrimes in Palestine. Per Palestinian police statistics in Ramallah, 2016 witnessed more than 1,200 cybercrimes compared to 520 in 2015, according to officer Louay Azriqat, the spokesman for the Palestinian police in Ramallah." READ MORE

Source: 242Viral

Date: 26 Jan 2017

Budapest Convention on Cybercrime in The Bahamas

"[…] In order to become a member of the Convention, several steps need to be followed. Regulations are defined and characterized in the text of the Convention. Some of these provision have already been adopted in Bahamas. For example, The Computer Misuse Act 2003 and Data Protection Act 2003 were adopted and implemented from the initiative of Bahamas government. These acts bear much resemblance with Budapest Convention, although not all points are included." READ MORE

Source: Interpol

Date: 16 Jan 2017

Digital currencies and money laundering focus of INTERPOL meeting

"The threats posed by transnational criminal networks exploiting digital currencies for money laundering and terrorism financing are high on the agenda of an INTERPOL meeting in Qatar. […] Through the INTERPOL Global Complex for Innovation in Singapore, several projects related to the use of digital currencies such as Bitcoin for criminal purposes are being undertaken in partnership with law enforcement, international organizations and the private sector. These include projects on Bitcoin laundering and Blockchain analytics, in order to strengthen member countries' capabilities in this field." READ MORE

Source: Cameroon Info Net

Date: 27 Jan 2017

Cameroun, le site du Ministère de l'Enseignement supérieur piraté

"Ayant revendiqué ce piratage, les hackers disent être originaires des Régions anglophones. Ils laissent entendre par leur action qu'ils ne peuvent plus rester insensibles aux mauvais traitements infligés par les pouvoirs publics à leurs frères du Sud-Ouest et du Nord-Ouest. C'est une information que relaie le quotidien Le Jour édition du 27 janvier 2017. En date du 25 janvier 2017, le site internet du Ministère de l'Enseignement supérieur a été victime d'un piratage. Ce qui explique la raison pour laquelle il demeure depuis le jour de cette attaque indisponible. Des colonnes de nos confrères, on apprend que la menace a été revendiquée par un groupe baptisé Cameroon Cyber Force (CCF). Ce dernier avait alors posté sur le site du MINESUP un message en anglais «qui a été retiré par la suite», précise le quotidien." READ MORE

Source: The New Times

Date: 23 Jan 2017

How Police tracked and foiled $700,000 bank robbery in Rwanda

"Last year, a gang comprised Rwandans and foreigners hatched a plan to hack into the international transaction system of a local commercial bank to steal $700,000. The money was to be transferred from accounts of five public institutions hosted by the targeted bank, and wired to an account in another country. […] However, the theft was foiled by the Rwanda National Police cyber investigation unit the day the transaction was to be carried out, apparently by a hacker, who was based outside the country. […] The operationalisation of the 'Regional Cyber Crime Centre of Excellence' currently under construction, which will be connected to the Cyber Crime Centre of Lyon and The Interpol Global Complex for Innovation in Singapore, will further supplement other initiatives like the national forensic laboratory and bilateral and multilateral cooperation, to ensure a solid platform against IT-facilitated crimes." READ MORE

Latest reports

- ENISA, Report on Blockchain Technology and Security, 18 Jan 2017
- White House, Privacy in our digital lives: Protecting Individuals and Promoting Innovation, Jan 2017
- ENISA, A good practice guide of using taxonomies in incident prevention and detection, 30 Jan 2017
- GCSCC, New Report Pokes Holes in Uganda's Cyber Security Capacity, 25 Jan 2017
- FireEye, 2017 Cyber Threats: A perfect storm about to hit Europe?, January 2017
- HelpNet Security, Data breaches hit all-time record high, increase 40% in 2016, 20 Jan 2017
- PaloAlto Networks, Exploring the Cybercrime Underground: Part 3 – Into the RAT Nest, 26 Jan 2017

Upcoming events

- 3 Feb 2017, The Hague, the Netherlands – Participation in the Task Force on cybercrime meeting at EUROJUST, GLACY+
- 8–10 Feb 2017, Kyiv, Ukraine – Seminar on communication and information sharing with local ISPs, combined with workshop on legal amendments related to cybercrime and electronic evidence, EAP III
- 13–15 Feb 2017, Baku, Azerbaijan – Workshop on reform of legislation to ensure compliance with Art. 16 and Art. 17 of Budapest Convention, EAP II
- 13–15 Feb 2017, Guatemala City, Guatemala – Advisory mission on legislation on Cybercrime and electronic evidence in line with the Budapest Convention, GLACY+
- 16 Feb 2017, Sarajevo, Bosnia and Herzegovina – Advice and workshop on the preparation of interagency cooperation protocols, iPROCEEDS