Cybercrime Digest

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

1-15 March 2017

Source: Council of Europe

Date: 1 Mar 2017

The Cybercrime Convention Committee (T-CY) adopts Guidance Note on Article 18 Budapest Convention

"The Cybercrime Convention Committee, following detailed negotiations, has adopted a Guidance Note on the production of subscriber information following a lawful request by a criminal justice authority. This includes situations where a service provider is offering a service in the territory of a State without necessarily being located in the State or where the subscriber information sought may be stored in another jurisdiction or on servers "somewhere in the cloud"." READ MORE

RELATED ARTICLES

Council of Europe, Guidance Note #10 on Production Orders, 1 Mar 2017

Source: INTERPOL

Date: 3 Mar 2017

Cybercrime investigation challenges focus of Council of Europe and INTERPOL initiative

"Building capacity and enhancing cooperation in cyber investigations around the world is the focus of a joint initiative between INTERPOL and the Council of Europe. With the rapid growth in the number and sophistication of cyber-related offences, electronic evidence gathering presents significant transnational policing challenges which require effective cooperation at all levels: police-to-police, police-to-judicial authorities and police-to-service providers. The Global action on Cybercrime extended (GLACY+) project, funded by the European Union and the Council of Europe, will help investigators and prosecutors identify and address issues relating to delays in information exchange, coping with diverse legislative and policy frameworks, and collaboration with the private sector." READ MORE

Source: Agence de Presse Senegalaise

Date: 14 Mar 2017

La lutte contre la cybercriminalité doit intégrer "la primauté du droit"

"La lutte contre la cybercriminalité doit préserver "la primauté du droit", a souligné, mardi, le conseiller, chef de la section économie, commerce et gouvernance à la Délégation de l'Union européenne à Dakar, Clemens Schroeter. […] M. Schroeter s'exprimait à l'ouverture d'un cours de formation sur la cybercriminalité et la preuve électronique, à l'intention de juges et procureurs des pays francophones et lusophones de la région ouest-africaine plus la Mauritanie. […] Ce cours organisé par Action globale sur la cybercriminalité élargie (GLACY+, en anglais), a pour objectif de permettre aux participants d'acquérir des connaissances juridiques de base sur la cybercriminalité et la preuve électronique." READ MORE

Source: Europol

Date: 14 Mar 2017

Credit card fraud in 130 000 cases: Organised crime group disrupted in European cross-border action

"The Cypriot Police with the support of Europol, the US Secret Service and the Investigative Committee of the Republic of Belarus, have disrupted an organised

criminal group that affected more than 130 000 payment card holders from 29 countries. Financial losses, including those for EU citizens, totalled EUR 8 million. Four members of the criminal organisation, including the leader, were identified and arrested during a police raid in Belarus. The first court proceeding in this case has led to a sentence of up to 7 years of imprisonment." READ MORE

Source: Europol

Date: 3 Mar 2017

Unique Police2Peer initiative combats child sexual exploitation and abuse online

"Peer-to-peer file sharing makes the collecting and sharing of child sexual abuse material online easy. Law enforcement all over Europe and their partners, with the support of Europol and EMPACT are now using those same networks to combat the illegal distribution of these files by sending a message to their users. This Police2Peer action will spread a unique new message about the consequences for users when illegal child abuse files are shared." READ MORE

Source: Newsweek

Date: 2 Mar 2017

DDoS attack takes down Luxembourg government servers

"The Luxembourg government's servers were hit by hackers in a massive DDoS attack that reportedly lasted over 24 hours. The attack, which began on Monday morning (27 February), is believed to have affected over a hundred websites hosted by the government's servers. […] According to local reports, attribution was difficult as those investigating the incident believe that the attack may have launched leveraging botnets." READ MORE

Source: SRF

Date: 9 Mar 2017

Soziale Netzwerke sollen mit Behörden kooperieren [Social networks should cooperate with authorities]

"Niederlassungen von sozialen Netzwerken wie Facebook Schweiz sollen in Zukunft mit den Strafverfolgungsbehörden kooperieren müssen. Dies verlangt eine Ständeratsmotion. Der Bundesrat hingegen setzt auf internationale Abkommen." READ MORE

Source: The Huffington Post

Date: 7 Mar 2017

African Governments Versus Social Media: Why The Uneasy Relationship?

"The list of African countries that have blocked access to social media during elections and other politically sensitive periods is growing. Over the past year this included; Cameroon, Chad, the Democratic Republic of Congo, Gabon, Gambia, the Republic of Congo and Uganda. Countries like Ethiopia, Madagascar and Tanzania, have introduced cybercrime legislation that threatens freedom of expression. Elsewhere, social media users, including journalists, have been prosecuted under existing legislation for content they have shared online." READ MORE

Source: Interpol

Date: 9 Mar 2017

Cybercrime underground economy emerging in West Africa

"A joint INTERPOL and Trend Micro research paper on cybercrime activity across West Africa has revealed a significant growth in cyber frauds on individuals and businesses.

Combining survey results from INTERPOL member countries across the region with research findings by Trend Micro, the 'Cybercrime in West Africa: Poised for an Underground Market' paper shows West African cybercriminals are increasingly using social engineering tactics. The survey showed an increase of 132 per cent of reported cybercrime between 2013 and 2015, with an average of USD2.7 million from business and USD422,000 from individuals stolen each year. However an average of 30 per cent of cybercrimes reported to law enforcement in the region over the same period resulted in arrests. The paper shows two major types of threat actors are active throughout the region – so-called 'Yahoo boys' and 'Next-Level Cybercriminals'." READ MORE

Source: Nairobi News

Date: 9 Mar 2017

Kenyan Police bust ring of bank hackers involved in multi-million thefts in Nairobi

"Kenya Revenue Authority, several blue-chip banks, a parastatal and a supermarket chain are some of the institutions penetrated by an international cybercrime syndicate that took off with hundreds of millions of shillings – before they were all seized on Monday and Tuesday. Working with insiders and relatives of "prominent politicians", the crooks had formed an international band that installed malware into the systems that allowed them to take control of the institutions' computers and steal what police sources said would run into hundreds of millions. On Monday night, police detectives from the Special Crime Prevention Unit, SCPU, and the Flying Squad smashed the syndicate and arrested a former police officer, a Kenya Revenue Authority employee and two American citizens who are now among 16 suspects in police custody for transnational crimes — that include cybercrime and drug trafficking." READ MORE

Source: Gadgets 360

Date: 15 Mar 2017

Twitter Confirms Top Accounts Hacked

"Several top Twitter accounts, including those of a German football club, a French ministry and BBC North America, were defaced Wednesday by pro-Turkish hackers with a message slamming "Nazi Germany" and "Nazi Holland". "#NaziGermany. #NaziHolland. This is a small #Ottomanslap for you. See you on #April16. I wrote what? Learn Turkish," read the message, which comes in the midst of a bitter row between Europe and Turkey over Turkish gov. rallies on European soil." READ MORE

Source: The Philippine star

Date: 6 Mar 2017

Cybercrime cases rising in the Philippines

"Cybercrime cases continue to rise with the upsurge in the number of internet users in the country, the Philippine National Police (PNP) said yesterday. Senior Superintendent Marni Marcos Jr., acting director of the Anti-Cybercrime Group (ACG), urged victims of online scams to report to authorities. "Victims may also file their complaints through www.pnpacg.ph, hotline number 7230401 local 5313 or e-mail at pnp.anticybercrimegroup@gmail.com," Marcos said. The ACG has recorded 555 cases of online schemes such as swindling, libel, threat, video voyeurism, identity theft and hacking since 2016." READ MORE

Source: Lexology

Date: 10 Mar 2017

Singapore Ministry of Home Affairs proposes changes to Computer Misuse and Cybersecurity Act

"The Bill seeks to extend the reach of the CMCA by criminalising acts which are enabled by cybersecurity attacks. In this regard, it would be an offence to use personal data

obtained via an act in breach of the CMCA. For example, it would be unlawful for a person to use hacked credit card details, even if the act of hacking was committed by another. In addition, the Bill also targets acts which enable cybercrime, by criminalising the act of obtaining and the act of dealing in tools which may be used to commit a CMCA offence. This would include hacking tools such as malware." READ MORE

Source: CXO Today

Date: 11 Mar 2017

India to introduce the Examiner of the Electronic Evidence to facilitate cybercrime investigations

"In a move to facilitate speedy prosecution of cybercrime and financial fraud cases, the government recently announced that it would appoint Examiner of Electronic Evidence (EEE) under section 79A of the IT Act 2000, to authenticate electronic evidences in the court. With the appointment of EEE, the government aims at eliminating the present hurdles in collecting, analyzing and proving digital evidences in the court of law. Since digital forensics is a crucial element in the cybercrime investigations, cyber security analysts expect that EEE will improve the present state of digital forensics mechanism in India. However, scarcity of manpower, lack of infrastructure and awareness are the major hurdles EEE will have to overcome for ensuring justice to victims." READ MORE

Source: HRN

Date: 3 Mar 2017

El secuestro de datos es la tendencia cibercriminal de 2017 en Colombia

"Según el estudio Consumer Security Risks Survey 2016 de Kaspersky Lab, en el que se tuvieron en cuenta los resultados de una encuesta realizada en Brasil, Colombia, México, entre otros 18 países, el 52% de los usuarios que sufrió pérdidas financieras a causa de ataques cibernéticos logró recuperar sólo una parte o nada. Por esto, Microsoft, como proveedor de servicios en la nube, y la Dirección de Investigación Criminal e Interpol (Dijin), manifestaron que la empresa estadounidense y las autoridades colombianas vienen realizando alianzas para combatir la cibercriminalidad y promover la protección de la privacidad de los datos. Hoy, tanto la Policía como Microsoft hacen un llamado a la ciudadanía para reducir los riesgos de los ciberataques y revelan las dos modalidades de secuestro de datos que tienen en jaque a los usuarios de la tecnología este año." READ MORE

Source: SC Media

Date: 2 Mar 2017

Howard Schmidt leaves indelible influence on cybersecurity

"Howard A. Schmidt, former White House cybersecurity coordinator, passed away Thursday. His accomplishments and influence over a more than 40-year tenure in cybersecurity, defense and law enforcement are too numerous and expansive to recount in such limited space. […] Schmidt did not simply pioneer cybersecurity – he continued to whisper to government, private industry, law enforcement authorities and even the president, where, as cybersecurity coordinator and special assistant to the president, he coordinated "interagency cybersecurity policy development and implementation," as well as engagement with federal, state, local, international, and private sector cybersecurity partners," whitehouse.gov said." READ MORE

Latest reports

- Europol, Crime in the age of technology – Europol's Serious and Organised Crime Threat Assessment 2017, 9 Mar 2017
- Europol/ Eurojust, Common challenges in combating cybercrime as identified by Eurojust and Europol, 2 Mar 2017
- ENISA, Guidelines on Incident Notification for Digital Service Providers, 28 Feb 2017
- UN Human Rights Council, Report of the Special Rapporteur on the right to privacy, 24 February 2017
- P. Pawlak, P.-N. Barmpaliou, Politics of cybersecurity capacity building: conundrum and opportunity, Journal of Cyber Policy, 7 Mar 2017
- RAND, Zero Days, Thousands of Nights, 8 Mar 2017
- F-Secure, State of Cyber Security 2017, Mar 2017

Upcoming events

- 15 – 16 March 2017, Tirana Albania - Workshops on inter-agency and international cooperation for search, seizure and confiscation of online crime proceeds, iPROCEEDS
- 15 – 16 March 2017, Ankara, Turkey, Advisory mission and workshop on online fraud and other cybercrime reporting mechanisms, iPROCEEDS
- 23 – 24 March 2017, Minsk, Belarus, Public-Private cooperation: Public-private partnerships in sector-specific approach, EAP III
- 23 – 24 March 2017, Port Louis, Mauritius - Study visit of the Philippines delegation to Mauritian CERT, GLACY+
- 27 – 30 March 2017, Tbilisi, Georgia, Training of law enforcement and prosecution services in international cooperation on electronic evidence/multinational providers cooperation, EAP II/EAP III
- 29 – 31 March 2017, Accra, Ghana – International workshop on criminal justice statistics on cybercrime and electronic evidence, GLACY+
- 30 – 31 March 2017, Panama City - Advisory mission on legislation on Cybercrime and Electronic Evidence , GLACY+
- 31 March - 2 April 2017, Colombo, Sri Lanka – Introductory Judicial training on Cybercrime and Electronic Evidence for Prosecutors, 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