Cybercrime Digest

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

16-30 September 2017

Source: Council of Europe

Date: 19 Sep 2017

1st Meeting of the T-CY Protocol Drafting Group

"On 19 and 20 September 2017, the first meeting of the T-CY Protocol Drafting Group was held in Strasbourg. This session marked the start of the work on the draft Second Additional Protocol to the Convention on Cybercrime (ETS 185), aimed at addressing the issue of access to electronic evidence in the cloud for criminal justice purposes. 44 experts from 28 countries and the European Commission, among other things, discussed an initial inventory of provisions to be developed. They also confirmed that the views of civil society, data protection organisations and industry will be sought in this process which is expected to last until the end of 2019." READ MORE

RELATED ARTICLES

Electronic Frontier Foundation, The Cybercrime Convention's New Protocol will uphold Human Rights, 18 Sep 2017

Source: Europol

Date: 18 Sep 2017

2017, the year when cybercrime hit close to home

"The past 12 months have seen a number of unprecedented cyber-attacks in terms of their global scale, impact and rate of spread. Already causing widespread public concern, these attacks only represent a small sample of the wide array of cyber threats we now face. Europol's 2017 Internet Organised Crime Threat Assessment (IOCTA) identifies the main cybercrime threats and provides key recommendations to address the challenges. […] The report highlights important developments in several areas of cybercrime:

- Ransomware has eclipsed most other cyber-threats with global campaigns indiscriminately affecting victims across multiple industries in both the public and private sectors. Some attacks have targeted and affected critical national infrastructures at levels that could endanger lives.
- The first serious attacks by botnets using infected insecure Internet of Things (IoT) devices occurred.
- Data breaches continue to result in the disclosure of vast amounts of data, with over 2 billion records related to EU citizens reportedly leaked in 12 months.
- The Darknet remains a key cross-cutting enabler for a variety of crime areas. It provides access to, amongst other things: the supply of drugs and new psychoactive substances; the supply of firearms for terrorist acts; compromised payment data to commit payment fraud; and fraudulent documents to facilitate fraud, trafficking in human beings and illegal immigration.
- Offenders continue to abuse the Darknet and other online platforms to share and distribute child sexual abuse material.
- Payment fraud affects almost all industries, having the greatest impact on the retail, airline and accommodation sectors.
- Direct attacks on bank networks to manipulate card balances, take control of ATMs or directly transfer funds, known as payment process compromise, represents one of the serious emerging threats in this area." READ MORE

Source: European Commission

Date: 18 Sep 2017

'Strengthening the stability and international security of cyberspace', Commissioner Avramopoulos at the UN General Assembly

"Cybersecurity is a responsibility for all of us. […] Just think that 95% of successful attacks are said to be enabled by "some type of human error – intentional or not". Cyber-hygiene for all therefore: awareness-raising, communication, training, skills-building, these are crucial and should be our priorities. The second major pillar is deterrence. Successful deterrence requires effective detection, traceability, investigation and prosecution. We will only begin to turn the tide on cyber-attacks, when we increase the chances of criminals getting caught and sanctioned for committing them. Here, the Council of Europe Budapest Convention on Cybercrime, is the cornerstone of our international partnership to exchange information and electronic evidence. This is of course linked to the third pillar of our strategy: global cooperation, which is in my view the most critical – and the most relevant to our context this week at the United Nations. […] The European Union will continue to advocate strongly that international law applies in cyberspace." READ MORE

Source: U.S. Department of Justice

Date: 26 Sep 2017

U.S. Deputy Attorney General delivers remarks to the Interpol 2017 General Assembly

"[…] We must all ensure that our countries are availing themselves of existing multilateral instruments and mechanisms to fight cybercrime. I call on all nations that have not already done so to consider joining the Budapest Convention on Cybercrime. It is a highly effective convention that ensures that cybercrime is subject to effective criminal sanctions in each country and that a mutual legal assistance relationship exists among all member countries. In addition, I urge countries to join the 24/7 High Tech Network, which ensures that critical cyber evidence can be preserved for use in investigations and prosecutions." READ MORE

Source: Council of Europe

Date: 26 Sep 2017

Enhancing the Network of 24/7 Contact Points

"The Council of Europe on 26 and 27 September held a meeting of the 24/7 Network of Contact Points at EUROPOL, The Hague. Fifty-five representatives of contact points of 45 current and future Parties to the Budapest Convention from all regions of the world shared best practices in view of further enhancing the role and effectiveness of the network. The Network has been established under Article 35 of the Budapest Convention on Cybercrime." READ MORE

Source: INTERPOL

Date: 25 Sep 2017

Millions of medicines seized in largest INTERPOL operation against illicit online pharmacies

"In the largest action of its kind, INTERPOL's Operation Pangea X targeting the illicit online sale of medicines and medical devices saw some 400 arrests worldwide and the seizure of more than USD 51 million worth of potentially dangerous medicines. Involving 197 police, customs and health regulatory authorities from a record 123 countries, Operation Pangea X led to 25 million illicit and counterfeit medicines seized worldwide. The action resulted in 1,058 investigations, 3,584 websites taken offline and the suspension of more than 3,000 online ads for illicit pharmaceuticals." READ MORE

Source: Ministerio Publico de Gobierno, Panama

Date: 27 Sep 2017

Panamá, MP presenta proyecto de ley que modifica y adicionada artículos al Código Penal relacionados al Cibercrimen

"Los delitos informáticos o cometidos a través de medios cibernéticos, son modalidades delictivas, que a través de los años han modificado el modo de operación, generando delitos de acoso, pornografía infantil, estafas, entre otros. En virtud de ello, la Procuraduría General de la Nación presentó hoy, ante el Pleno de la Asamblea Nacional el Proyecto de Ley "Que modifica y adiciona artículos al Código Penal, relacionados con el Cibercrimen". […]Es necesario que Panamá cuente con ellas toda vez que así nos adecuamos a las exigencias internacionales y al Convenio de Budapest de 2001, sobre la Ciberdelincuencia del cual somos signatarios, concluyó diciendo." READ MORE

Source: Government of Norway

Date: 27 Sep 2017

Norwegian Government launches first international cyber strategy

"Norway's first international cyber strategy was launched in Oslo at the annual dialogue meeting on international cyber issues between the US and the Nordic and Baltic countries. The strategy sets out Norway's governing principles and strategic priorities relating to the whole spectrum of international cyber policy issues: cyber security, innovation and the economy, international cooperation to combat cybercrime, security policy, global governance of the internet, development and human rights." READ MORE

Source: Biznis Vesti

Date: 21 Sep 2017

iPROCEEDS, simulation exercise to fight cybercrime in "the former Yugoslav Republic of Macedonia"

"Cybercrime investigators, digital forensics specialists, financial investigators, prosecutors, Financial Intelligence Unit as well as representatives of the Directorate for Personal Data Protection (DPA), from "the former Yugoslav Republic of Macedonia" has gathered today to participate in a four days Cybercrime Simulation Exercise, in Skopje. The activity is organised by the Cybercrime Programme Office of the Council of Europe, through the joint project of European Union and the Council of Europe – iPROCEEDS, from 25 to 28 September 2017." READ MORE (in Macedonian); VIDEO (in Albanian)

Source: The Indian Express

Date: 21 Sep 2017

Indian Government plans Bill with more teeth to tackle cyber crimes

"The government plans to bring a digital payment Bill to strengthen legal framework and enhance surveillance to check cybercrimes in the financial sector, including frauds targeting cards and e-wallets, said officials. The feasibility of such legislation, according to officials, was discussed during a meeting chaired by Union Home Minister Rajnath Singh on Tuesday. According to officials, an inter-ministerial committee headed by the home minister will first study existing laws to deal with cybercrimes and then propose new legislation, said an official, adding that the need was felt after a spurt in the number of complaints, especially after demonetisation. The proposed legislation will not only deal with punishment and fine for those who dupe online users, it will have measures to fix responsibility in cases where digital transactions land in any dispute." READ MORE

Source: Xinhua Net

Date: 20 Sep 2017

ASEAN, dialogue partners call for closer counter-terror cooperation

"The 10 member states of the Association of Southeast Asian Nations (ASEAN) and its dialogue partners China, Japan and South Korea on Thursday called for closer regional cooperation to combat terrorism and violent extremism. […] On cybercrime, Philippine Interior and Local Government officer-in-charge Catalino Cuy said the ministers also endorsed the ASEAN Declaration to Prevent and Combat Cybercrime, which includes measures such as acknowledgment of the importance of harmonization of laws related to cybercrime and electronic evidence, and encouragement of ASEAN member states to explore the feasibility of acceding to existing regional and international instruments in combating cybercrime, to name a few." READ MORE

Source: Singapore Government

Date: 18 Sep 2017

Singapore signs Memorandum of Cooperation on Cybersecurity with Japan

"Singapore and Japan today signed a Memorandum of Cooperation (MOC) to strengthen cybersecurity cooperation between the two countries. The MOC was signed by Mr David Koh, Chief Executive, Cyber Security Agency of Singapore, and Dr Ikuo Misumi, Deputy Director-General of the National Center of Incident Readiness and Strategy for Cybersecurity, Japan. The MOC covers cybersecurity cooperation in key areas including regular policy dialogues, information exchanges, collaborations to enhance cybersecurity awareness, joint regional capacity building efforts, as well as sharing of best practices between both countries." READ MORE

RELATED ARTICLES

Channel NewsAsia, Singapore's Cybersecurity Bill delayed to 2018, 18 Sep 2017

Source: Turkish Minute

Date: 26 Sep 2017

Turkey, Supreme Court rules on ByLock in line with Justice Minister's remarks

"The Supreme Court of Appeals' Assembly of Criminal Chambers has ruled the ByLock smart phone application to be considered evidence of membership in a terrorist organization following Turkish Justice Minister Abdülhamit Gül's remarks on ByLock being strong evidence of terrorist organization membership. According to the decision, ByLock will be considered evidence in and of itself for prosecution on charges of membership in the Gülen movement, accused by the government of mounting a botched coup attempt in July 2016." READ MORE

Source: Reuters

Date: 26 Sep 2017

Russia tells Facebook to localize user data or be blocked

"Russia will block access to Facebook next year unless the social network complies with a law that requires websites which store the personal data of Russian citizens to do so on Russian servers, Russian news agencies reported on Tuesday. The threat was made by Russia's communications watchdog Roskomnadzor, agencies said, the organization which blocked access to LinkedIn's website last November in order to comply with a court ruling that found the social networking firm guilty of violating the same data storage law." READ MORE

Source: Kyiv Post

Date: 22 Sep 2017

Belarus preparing new Internet restrictions

"Belarus is going to make adjustments to the documents that regulate the Internet, Belarusian Communications and Informatization Minister Sergei Popkov said. "There will be nothing super-tough […] You know that it's impossible to close the Internet […] There are absolutely no new approaches here […] All countries have the same approaches now: to protect citizens against the influence of negative information as much as possible," Popkov told a press conference in Minsk. The document in question is the presidential decree on the improvement of the procedures for using the information space. […] The minister said the document may be drafted before the end of this year." READ MORE

Source: RadioFreeEurope RadioLiberty

Date: 26 Sep 2017

Iran Charges Telegram Management Over Extremism, Pornography Allegations

"Iranian news agencies say Tehran's prosecutor has filed criminal charges against the "management" of Telegram, the popular encrypted messaging app founded by Russian social-networking mogul Pavel Durov. Prosecutor Abbas Jafari Dolatabadi said that the charges stemmed from Telegram's alleged role as a platform for child pornography and extremist content, including by Islamic State militants. The reports on September 26 by the semiofficial ISNA news agency and the judiciary's Mizan news agency did not name specific individuals implicated in the case." READ MORE

Source: The New York Times

Date: 25 Sep 2017

China blocks WhatsApp, broadens online censorship

"China has largely blocked the WhatsApp messaging app, the latest move by Beijing to step up surveillance ahead of a big Communist Party gathering next month. The disabling in mainland China of the Facebook-owned app is a setback for the social media giant, whose chief executive, Mark Zuckerberg, has been pushing to re-enter the Chinese market. WhatsApp was the last of Facebook products to still be available in mainland China; the company's main social media service has been blocked in China since 2009, and its Instagram image-sharing app is also unavailable." READ MORE

Source: Defi Media

Date: 18 Sep 2017

Cybercriminalité: Maurice sous la menace d'une intensification

"Internet est devenu un vaste champ d'action dont les visiteurs ignorent les dangers. Piratage, vol d'identité, « cyber bullying » et sextorsion sont courants. Depuis le début de l'année, la Cybercrime Unit a enregistré une vingtaine de cas chaque mois. Les autorités tentent de s'attaquer au problème." READ MORE

Source: Lactuacho

Date: 29 Sep 2017

Près de 45% des grandes entreprises en Afrique de l'Ouest piratées

"Près de 45% des grandes entreprises de l'espace ouest-africain sont piratées, a annoncé, jeudi, Mack Coulibaly, directeur général de JIGHI INC, au lancement, à Abidjan de la deuxième édition l'Africa Cyber Security Conference. Selon M. Coulibaly, les cyberattaques et la vulnérabilité du cyber espace constituent une menace réelle pour les économies africaines fragiles." READ MORE

Source: Quartz Africa

Date: 21 Sep 2017

WhatsApp's role as a government protest tool is in the spotlight again as Togo blocks it

"The internet has been intermittent in Togo with the government blocking access to social media networks and shutting down mobile messaging, activists in the country have confirmed to Quartz. The slowdown started on Tuesday night (Sept. 19) after opposition members boycotted a parliamentary session that proposed changes to presidential term limits and called for protests on Wednesday and Thursday. Anti-government protests have spread across Togo in recent weeks calling for president Faure Gnassingbé to step down and allow constitutional reforms." READ MORE

Source: Matangi Tonga Online

Date: 25 Sep 2017

Tonga, fighting cybercrime requires regional and international cooperation

"Cooperation at regional and international level is essential for fighting the unique challenges cybercrime presents to the peoples of the Pacific and the entire world, Tonga's Lord Chief Justice O.G Paulsen told the opening of the five-day, 'Introductory Training of Trainers Course on Cybercrime and Electronic Evidence for the Pacific', implemented by the Council of Europe. […] Government and law enforcement in Tonga saw the need to develop and update its legislation on electronic evidence and cyber related crimes. Tonga realized it must bring its laws in line with the world's practices. This is a major reason why just this year Tonga acceded to and ratified the Budapest Convention." READ MORE

Source: The Island Sun

Date: 20 Sep 2017

Solomon Islands vulnerable to cyber crime

"Speaking during the national workshop on promoting information and communication awareness on cybercrime and laws, Mr Ronald Bei Talasasa said Solomon Islands does not have a stand-alone legislation to deal with cyber-crime. There is an international law called Budapest Convention that has been endorsed to penalise cybercrime, but Solomon Islands is unable to act upon it because of our lack in law to deal with the crime. Mr Talasasa explained that DPP can only prosecute crime committed using ICTs based on what is available in the country's penal code. […] Mr Talasasa said political will is crucial in making sure the country has a cyber-crime legislation put in place to guide users of ICT. […] Mr Talasasa said the process will be long and challenging but through cooperation and working together, the country will soon have legislation to prosecute cyber-crime." READ MORE

Source: The Guardian

Date: 25 Sep 2017

Deloitte hit by cyber-attack revealing clients' secret emails

"One of the world's "big four" accountancy firms has been targeted by a sophisticated hack that compromised the confidential emails and plans of some of its blue-chip clients, the Guardian can reveal. Deloitte, which is registered in London and has its global headquarters in New York, was the victim of a cybersecurity attack that went unnoticed for months. The Guardian understands Deloitte clients across all of these sectors had material in the company email system that was breached. The companies include household names as well as US government departments." READ MORE

Latest reports

- Council of Europe, Summary report of the 1st Meeting of the T-CY Protocol Drafting Group, 20 Sep 2017
- Europol, 2017 Internet Organised Crime Threat Assessment, 27 Sep 2017
- UK Parliament, Data Protection Bill, September 2017
- Singapore CERT, Overview of cyberthreats 2016, 16 Sep 2017
- Twitter, New Data, New Insights: Twitter's Latest #Transparency Report, 19 Sep 2017
- Europol's European Cybercrime Centre (EC3) and Trend Micro Forward-Looking Threat Research (FTR) Team, Cashing in on ATM Malware, 26 Sep 2017

Upcoming events

- 3-4 October, New Delhi, India – CyFy: The India Conference on Cyber Security and Internet Governance, Cybercrime@Octopus
- 3-5 October, Alexandria, Virginia, US – Participation of two delegates from the Philippines in the Cybertipline Roundtable, GLACY+
- 4-5 October, Ljubljana, Slovenia – Regional workshop to share experience on indicators and guidelines for financial sector entities to prevent money laundering in the online environment in cooperation with FIU Slovenia, iPROCEEDS
- 6 October, Kyiv, Ukraine – Memorandum: contribution to IGF-UA, Cybercrime@EAP III
- 9-10 October, Kraków, Poland – Participation in the 3rd European Cybersecurity Forum (CYBERSEC), T-CY
- 9-11 October, Baku, Azerbaijan – Regional conference on cybercrime and money laundering in cooperation with the Global Prosecutor's E-Crime Network (GPEN) and the Government of Azerbaijan, iPROCEEDS, Cybercrime@EAP II
- 10 October, Tirana, Albania – Workshop of the working group to elaborate guidelines and indicators for financial sector entities to prevent money laundering in the online environment, iPROCEEDS
- 10-13 October, Santo Domingo, Dominican Republic – Support to the national delivery of Intro Course on cybercrime and e-evidence for Judges and prosecutors, GLACY+
- 11-13 October, Port Louis, Mauritius – INTERPOL's 4th African Working Group Meeting on Cybercrime for Heads of Cybercrime Units, GLACY+
- 12 October, Podgorica, Montenegro – Workshop of the working group to elaborate guidelines and indicators for financial sector entities to prevent money laundering in the online environment, iPROCEEDS
- 12-13 October, Bucharest, Romania – Study visit of CERT representatives to CERT-RO, iPROCEEDS
- 12-13 October, Baku, Azerbaijan – Safeguards and operational agreements study visit, plus feasibility study and inventory of initiatives, Cybercrime@EAP III
- 13 October, Vienna, Austria – Support to Belarus to take part in Council of Europe/OSCE Internet Freedom Conference, Cybercrime@EAP III
- 13 October, Sarajevo, Bosnia and Herzegovina – Workshop of the working group to elaborate guidelines and indicators for financial sector entities to prevent money laundering in the online environment, iPROCEEDS
- 13-15 October, Kandy, Sri Lanka – Residential workshop for District Judges and Magistrates on cybercrime and electronic evidence – second batch, GLACY+