Cybercrime Digest

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

1-15 April 2017

Source: UNODC

Date: 5 Apr 2017

UN Expert Group on Cybercrime meets in Vienna

"The UN Intergovernmental Expert on Cybercrime will meet at the United Nations in Vienna from 10 to 13 April. The Council of Europe and members of the Cybercrime Convention Committee (T-CY) will use that opportunity to report on progress made under the Budapest Convention since the last meeting of the Group in 2013 and share experience on capacity building programmes." READ MORE

RELATED ARTICLES

EU/CoE, Information on EU/COE capacity building programmes, 5 Apr 2017

Source: EDRi

Date: 10 Apr 2017

Discussion on cross-border access to electronic evidence at RightsCon

"The bulk of the discussions focussed on a possible new protocol to the Cybercrime Convention of the Council of Europe (CoE). The CoE initiative is far broader than the Council of Europe area, covering all 53 countries that have ratified the Cybercrime Convention (including the USA, Australia, Canada and others). […] Alexander Seger opened by arguing that cross-border is a rather fictional concept on the internet. He said that the Cybercrime Convention is a criminal justice treaty, so data access is about access to specific data in specific criminal investigations, and not about bulk data collection or national security measures. All measures fall under criminal law, which is where countries have the strongest safeguards. In addition, the starting point in any such discussions is that, as detailed in the European Convention on Human Rights, there is a positive obligation on states to protect citizens from crime." READ MORE

Source: Europol

Date: 4 Apr 2017

No More Ransom adds 15 new decryption tools as record number of partners join global initiative

"The platform www.nomoreransom.org is now available in 14 languages and contains 40 free decryption tools. Since our last report in December, more than 10 000 victims from all over the world have been able to decrypt their affected devices thanks to the tools made available free of charge on the platform. No More Ransom was launched in July 2016 by the Dutch National Police, Europol, Intel Security and Kaspersky Lab, introducing a new level of cooperation between law enforcement and the private sector to fight ransomware together. Since the launch, dozens of partners from all continents have joined. This shows that ransomware is a worldwide problem that needs to be and will be fought together. Statistics show that most visitors to the platform come from Russia, the Netherlands, the United States, Italy and Germany." READ MORE

Source: Irish Legal News

Date: 13 Apr 2017

Irish cybercrime bill approved at second stage

"The first Irish legislation dealing with cybercrime was approved by Senators after its second stage debate in the Seanad yesterday. The Criminal Justice (Offences Relating to Information Systems) Bill 2016, which gives effect to EU directives and the Budapest Convention on cybercrime, will proceed to committee stage later this month.

Introducing the bill to the Seanad yesterday, Government minister David Stanton said: "The interconnection of computers and information systems, through cyberspace, facilitates communication between companies and individuals across the world. What has become clear is that, as cyberspace has developed and evolved, so has cybercrime which is a transnational phenomenon." READ MORE

Source: DN Portugal

Date: 15 Apr 2017

Portugal fez oito mil pedidos a Facebook, Google e Microsoft para combater cibercrime

"As autoridades portuguesas (Polícia Judiciária e Ministério Público) enviaram desde 2013 mais de oito mil pedidos diretamente ao Facebook, Microsoft e Google para obtenção de prova em casos de suspeitas de cibercrime. Crimes de natureza distinta mas com um ponto em comum: serem praticados através da internet ou por mera via informática. Casos de vendas online fraudulentas (que ocupam uma parcela significativa da cibercriminalidade), roubos de identidade, criação de perfis falsos no Facebook, pornografia infantil ou phishing bancário." READ MORE

Source: Euractiv

Date: 6 Apr 2017

Germany rolls out new cyber defense team

"Germany's army was targeted 284,000 times by cyber attacks in the first three months of 2017. Yesterday (5 April), the Bundesrepublik's new cyber defence unit was officially put into action. But its offensive capabilities are already under scrutiny. The new commando unit is set to be 13,500 personnel strong by July. By comparison, its marines corps has around 16,000 soldiers and the air force 28,000. Germany hopes to be a model for other European armed forces to follow in dealing with cyber attacks." READ MORE

Source: NATO

Date: 11 Apr 2017

US, Europe partner to counter 'fake news' and cyberattacks

"Several NATO Allies and European Union members came together in Helsinki on Tuesday (11 April 2017), formally agreeing to establish a European Centre of Excellence for Countering Hybrid Threats in the Finnish capital. […] In total, nine nations signed the Memorandum: Finland, France, Germany, Latvia, Lithuania, Poland, Sweden, the United Kingdom and the United States. Other NATO and EU nations are expected to join the Centre in the near future. While not signatories themselves, NATO and the EU will participate actively in the Centre's activities." READ MORE

Source: Business Wire

Date: 4 Apr 2017

Bitcoin and Crypto Currencies Take Center Stage at APWG Symposium on Electronic Crime Research

"Global cybercrime-fighting association APWG is hosting its eCrime 2017 conference on April 25-27 in Scottsdale, Arizona, USA. […] APWG Secretary General Peter Cassidy said, "Electronic crime succeeds ultimately through access to conventional banking services, where criminals can pay each other, or can extract stolen funds from victims. The 2017 eCrime conference will focus on the ability of industry and law enforcement to preserve its capacity to observe, respond and manage cybercrime mediated through the virtual currencies that are becoming ubiquitously fungible," Mr. Cassidy said." READ MORE

Source: Ghana National Communications Authority

Date: 3 Apr 2017

Ministers for Communication and National Security of Ghana pledge to support efforts against cybercrime

"The Honourable Ministers for Communications and the National Security, Mrs. Ursula Owusu-Ekuful and Mr. Albert Kan-Dapaah respectively, have pledged and reiterated government's support in the fight against cybercrime at an opening session of a Training of Trainers in Accra on Monday, 3rd April, 2017. The week-long course on Cybercrime and Electronic Evidence for judges and prosecutors is being held at the Judicial Training Institute (JTI) from the 3rd to 7th April, 2017 and is organised by the Council of Europe with the support of the National Communications Authority (NCA). It forms part of the Global Action on Cybercrime Extended (GLACY+) project. The main purpose of the training is to establish a group of trainers who will be able to instruct their peers in the introductory skills and knowledge required to fulfil their respective roles and functions in case of cybercrime and electronic evidence." READ MORE

RELATED ARTICLES

Ghana News Agency, Cybercrime major security threat in Ghana, 3 Apr 2017

Source: South China Morning Post

Date: 4 Apr 2017

Laws passed in Singapore to criminalise use of stolen personal data

"Laws were passed in Singapore to, among other things, make it illegal for individuals and businesses to make use of illicitly obtained personal data — including credit card or bank account information — as several Members of Parliament (MPs) raised concerns about the robustness of firms' cybersecurity measures. The MPs suggested making it mandatory for companies to report cyber attacks, and called for greater support for businesses to beef up their capabilities in dealing with such incidents. More individuals in both the public and private sectors should also be trained in cybersecurity, they said. Among the changes, the Computer Misuse and Cybersecurity Act was amended to stipulate that cyber criminals who launch attacks from abroad that cause "serious harm" to Singapore will be dealt with. The act of obtaining, making or supplying hacking tools such as physical devices or software was also made illegal." READ MORE

Source: Reuters

Date: 10 Apr 2017

Cyber attack on Union Bank of India similar to Bangladesh heist

"A cyber attack on Union Bank of India last July began after an employee opened an email attachment releasing malware that allowed hackers to steal the state-run bank's data, the Wall Street Journal reported on Monday. The attempt closely resembled the cybertheft last year of more than $81 million from the Bangladesh central bank's account at the New York Federal Reserve, the paper reported. The opening of the email attachment, which looked like it had come from India's central bank, initiated the malware that hackers used to steal Union Bank's access codes for the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a system that lenders use for international transactions." READ MORE

RELATED ARTICLES

Finextra, SWIFT introduces tool to help banks spot fraudulent messages, 12 Apr 2017

Source: Dark Reading

Cybercriminals seized control of Brazilian Bank for 5 Hours

Date: 4 Apr 2017

"Cybercriminals for five hours one day last fall took over the online operations of a major bank and intercepted all of its online banking, mobile, point-of-sale, ATM, and investment transactions in an intricate attack that employed valid SSL digital certificates and Google Cloud to support the phony bank infrastructure. The attackers compromised 36 of the bank's domains, including its internal email and FTP servers, and captured electronic transactions during a five-hour period on Oct. 22, 2016. Researchers estimate that hundreds of thousands or possibly millions of the bank's customers across 300 cities worldwide, including in the US, may have been victimized during the hijack window when customers accessing the bank's online services were hit with malware posing as a Trusteer banking security plug-in application." READ MORE

Source: Traveller 24

Cyber Scams: South Africa one of the top 10 most targeted countries

Date: 4 Apr 2017

"Card payments and data sharing within the travel and tourism industry are heavily under scrutiny as cyber-attacks, phishing scams and data breaches become more frequent and sophisticated. According to PCI Security Standards Council General Manager Stephen Orfei, South Africa's blossoming entrepreneurial landscape has unfortunately seen it become "one of the top ten markets targeted for cyber security weakness". […] As cyber-criminals continue to threaten the safety of payments, cyber-security skills are critically important to the payments industry used in all spheres as well as how data is securely stored, he says." READ MORE

Source: The Hacker News

Hackers Stole $800,000 From Russian ATMs With Disappearing Malware

Date: 3 Apr 2017

"Hackers targeted at least 8 ATMs in Russia and stole $800,000 in a single night, but the method used by the intruders remained a complete mystery with CCTV footage just showing a lone culprit walking up to the ATM and collecting cash without even touching the machine. Even the affected banks could not find any trace of malware on its ATMs or backend network or any sign of an intrusion. The only clue the unnamed bank's specialists found from the ATM's hard drive was — two files containing malware logs." READ MORE

Source: Threatpost

Spammer's arrest puts end to Kelihos botnet

Date: 11 Apr 2017

"The alleged Russian botmaster behind the Kelihos botnet was arrested while on vacation in Spain, putting an end to a seven-year cybercrime operation that foisted hundreds of millions of spam messages on consumers, as well as a dangerous array of banking malware and ransomware. Pyotr Levashov, also known as Peter Severa and a handful of other aliases, was arrested on Sunday by authorities in Barcelona. The U.S. Department of Justice yesterday released a statement acknowledging international cooperation between U.S. and foreign authorities, as well as the Shadow Server Foundation and Crowdstrike, in making the arrest and seizing infrastructure used to support Kelihos and Levashov's operations." READ MORE

Source: Diario Judicial

Date: 12 Apr 2017

Argentina, un voto no positivo a la pornografía infantil

"Julio Cobos, Senador por Mendoza, presentó un proyecto de ley para modificar el artículo 128 del Código Penal con la intención que la posesión de material pornográfico de menores sea delito, en conformidad con la adhesión al convenio sobre el Ciberdelito del Consejo de Europa. El ex vicepresidente de la Nación expresó que "es trascendental otorgar a la justicia las herramientas necesarias para poder actuar en temas tan importantes como el de la pornografía infantil". En cuanto al convenio sobre Ciberdelito europeo, Argentina adhirió a la Convención de Budapest, documento que incorpora dentro de los tipos de conductas criminalizadas la acción de poseer material pornográfico que incluye a niños. En ese marco, el Senador sostuvo que "el mismo establece que todo Estado parte debe adoptar medidas para que, como mínimo, los actos y actividades que el protocolo enumera queden íntegramente comprendidos en la legislación penal." READ MORE

Source: ICT Pulse

Date: 8 Apr 2017

Cyber Threats and Security in the Caribbean in 2017

"[…] The response to these issues across CARICOM and the broader region is (still) severely lacking. For one, the vast majority of the countries in the Caribbean do not have a national cyber crime strategy. This includes legislative reform (e.g. computer misuse, data protection, privacy, e-commerce, etc.), incident response capabilities, threat intelligence sharing, cybersecurity education & training, and other important elements. […] Regional leaders should now be looking towards options like signing on to the Budapest Convention and/or modeling new data protection laws on the EU's General Data Protection Regulations (GDPR)." READ MORE

RELATED ARTICLES

Loop News, Not enough done to tackle million dollar cybercrime industry, 6 Apr 2017

Latest reports

- Europol, Banking Trojans: From Stone Age to Space Era, 21 Mar 2017
- Art. 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Reg. 2016/679, 4 Apr 2017
- G7 Declaration On Responsible States Behavior In Cyberspace, 11 Apr 2017
- National Cyber Security Center UK, Cyber crime: understanding the online business model, April 2017
- Irish Department for Justice and Equality, Criminal Justice (Offences Relating to Information Systems) Bill 2016, 12 Apr 2017
- The Canadian Chamber of Commerce, Cyber Security in Canada: Practical Solutions to a Growing Problem, April 2017
- McAfee Labs, Threats Report 1Q2017, April 2017
- K. Bannelier, T. Christakis, Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors, 31 Mar 2017
- CGI and Oxford Economics, The Cyber-Value Connection, 12 Apr 2017

Upcoming events

- 19-20 April, Belgrade, Serbia - Advice and workshops on the preparation of interagency cooperation protocols and on domestic protocols for international sharing of intelligence and evidence, iPROCEEDS
- 24-28 April, Santo Domingo, Dominican Republic - Introductory Training of Trainers (ToT) on cybercrime and electronic evidence for Judges, Prosecutors and Lawyers, GLACY+
- 24-28 April, Manila, Philippines - Participation of one delegate from Ghana in the INTERPOL Malware Analysis Training, GLACY+
- 24-28 April, Tbilisi, Georgia - Regional case simulation exercise on cybercrime and financial investigations, EAP III / iPROCEEDS

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