Cybercrime Digest

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

1-15 November 2016

Source: Council of Europe

Date: 1 Nov 2016

Octopus Conference 2016: Cooperation against Cybercrime

“The 2016 edition of the Octopus Conference will be held on 16-18 November, in Strasbourg, France. The conference is organised by the Council of Europe, and will take place at the Palais de l'Europe. Under the theme 'Cooperation against Cybercrime', the conference will focus on two broad subjects: the Budapest Convention (and its 15th anniversary), and crime and jurisdiction in cyberspace - the way ahead. The three-day event will include workshops on:

- Service provider / law enforcement cooperation on cybercrime and electronic evidence
- Criminal justice access to evidence in the cloud: results of the Cloud Evidence Group
- Capacity building on cybercrime: lessons learnt
- The state of cybercrime legislation in Africa, Asia/Pacific and Latin America/Caribbean
- Terrorism and information technology: the criminal justice perspective
- International cooperation: enhancing the role of 24/7 points of contact
- Seeking synergies: Policies and initiatives on cybercrime of international and private sector organisations

The event will bring together cybercrime experts from public and private sectors, as well as international and non-governmental organisations.” READ MORE

Source: Europol

Date: 10 Nov 2016

Romanian operation supported by Europol leads to arrest of 24 cybercriminals

“On 9 November 2016, the Romanian Police and Prosecutor’s Office dismantled a large organised criminal group specialised in payment card fraud. Eighteen house searches were performed in six counties in Romania and 24 individuals were arrested. Electronic devices, computers, mobile phones and around EUR 50 000 in cash were seized, alongside evidence found in a criminal laboratory used for manufacturing skimming devices.” READ MORE

Source: IT Governance

Date: 1 Nov 2016

UK Government to launch £1.9bn cyber security strategy

“The Chancellor of the Exchequer, Philip Hammond, will today announce the UK’s new National Cyber Security Strategy, which aims to overhaul the country’s approach to cyber threats. According to the government’s April 2016 Annual Report on the 2011-2016 Cyber Security Strategy, the 2016-2021 Cyber Security Strategy will include £1.9 billion government investment “to provide the UK with the next generation of cyber security to defend our data, systems and networks, deter our adversaries, grow our cyber security sector and develop the critical capabilities that will make us a global leader in cyber security.” READ MORE

Source: National Cyber Security Centre – Ministry of Security and Justice, Netherlands

Date: 11 Nov 2016

Cyber Security Assessment Netherlands 2016: Professional criminals are an ever greater danger to digital security in the Netherlands

"Professional criminals are becoming increasingly better organized and are using advanced digital attack methods. In the past year, several large-scale attacks have taken place with a high degree of organisation, focusing on the theft of money and valuable information. In addition to the government, the victims were, increasingly, companies and private citizens. Professional criminals are thus, becoming a growing threat to the digital security in the Netherlands. That is apparent from the Cyber Security Assessment Netherlands 2016 (CSAN 2016) that State Secretary Dijkhoff presented to the Lower House in September and which is published in English today." READ MORE

Source: Daily FT

Date: 3 Nov 2016

Public-private partnerships key to mitigate cyber threats in Sri Lanka

"Telecommunication and Digital Infrastructure Minister Harin Fernando called for greater public-private partnerships to mitigate increasing cybercrimes and threats. "Today, critical infrastructures such as transportation, electricity, water supply and healthcare can be targeted by cybercriminals. All public and private institutions need to work together to form a public-private partnership for capacity building in law enforcement and the Judiciary as well as training and dealing better with cyber attacks." the Minister said at the Annual National Conference on Cyber Security." READ MORE

Source: ZD Net

Date: 2 Nov 2016

Tesco Bank says £2.5m was stolen from 9,000 customers in cyberattack

"A total of £2.5 million was stolen from 9,000 Tesco Bank customers in a sophisticated cyberattack last weekend, the bank has confirmed. The bank has also said that all account services have now returned to normal after all online transactions for all of its 136,000 current account holders were frozen following what the bank called "online criminal activity" spotted over the weekend." READ MORE

Source: Jamaica Information Service

Date: 9 Nov 2016

Cybercrime a Major Global Threat in Jamaica

"Minister of Justice, Hon. Delroy Chuck, says cybercrime is a major global threat that represents a clear and present danger to democracies and the rule of law everywhere. He said that cybercrime costs are projected to reach US$2 trillion worldwide by 2019 and the cybersecurity products and services market is expected to grow from US$75 billion in 2015 to US$175 billion by 2020. He said that in light of the challenges, societies cannot now afford for a fragmentation of cybercrime laws, divergence of procedural powers, lack of access to extraterritorial data by law enforcement authorities, and ineffective international cooperation mechanisms." READ MORE

RELATED ARTICLES

Jamaica Observer, Jamaica, cybercrime victims urged to report incidents, 2 Nov

Source: SC Magazine

Date: 11 Nov 2016

Russian banks suffer wave of DDoS attacks

"According to Russian media, five banks in the country have been subject to a swathe of DDoS attacks over the past few days. The state-owned Sberbank was one of them, and Kaspersky Lab said in a statement that the attacks were among the largest it had seen aimed at Russian banks." READ MORE

Source: South China Morning Post

Date: 2 Nov 2016

Sharp rise in Malaysian hacking cases

"There has been a sharp spike in computer hacking cases detected by CyberSecurity Malaysia over the past two years, says Malaysia's Science, Technology and Innovation Deputy Minister Datuk Dr Abu Bakar Mohamad Diah. "There were only three cases detected by MyCert in 2014. One involved Critical National Information Infrastructure (CNII) and two involved private companies," he said. "However, the number skyrocketed to a shocking 20 cases involving CNII, 43 private corporations, three higher learning institutions and 21 home users in 2015," he said." READ MORE

Source: The Hindu Business Line

Date: 11 Nov 2016

Indian Government to open cyber security centres

"Speaking at the Economic Editors' Conference here, Electronics and IT Minister Ravi Shankar Prasad said that his Ministry has approved 26 new posts in the Indian Computer Emergency Response Team (CERT-In) besides planning State CERT-Ins in five States. […] Three sectoral CERT-Ins in the power sector — generation, transmission and distribution — are also being set up in addition to one in the banking sector. "A national cyber coordination centre is being set up to provide real-time situational awareness and rapid response" Prasad said." READ MORE

Source: Reuters

Date: 7 Nov 2016

Controversial cybersecurity law adopted in China

"China adopted a controversial cyber security law on Monday to counter what Beijing says are growing threats such as hacking and terrorism, but the law triggered concerns among foreign business and rights groups. […] Overseas critics of the law say it threatens to shut foreign technology companies out of various sectors deemed "critical", and includes contentious requirements for security reviews and for data to be stored on servers in China. Rights advocates also say the law will enhance restrictions on China's Internet, already subject to the world's most sophisticated online censorship mechanism, known as the Great Firewall." READ MORE

Source: Albawaba

Date: 6 Nov 2016

Lebanon's lawmakers push for legislation overhaul to combat rising cybercrime

"Lebanon needs to pass new laws and upgrade existing legislations to check the rise of cybercrime phenomenon, a senior finance ministry official said Friday. "In order to improve the cybercrime fight, we need to make amendments to the existing laws and introduce new legislations to incriminate these types of electronic crimes. We also need to create awareness to about these types of crimes," Alain Bifani, the director general of the Finance Ministry, told participants in the cybercrime forum at the Coral Beach Hotel. Cybercrime has risen considerably in the past few years in Lebanon although the financial losses from this practice are not very substantial." READ MORE

Source: International Business Times

Date: 4 Nov 2016

Massive 'test' cyberattacks using Mirai botnet temporarily knock out Liberia's internet

"The same deadly malware behind the historic internet outage in the US in October seems to have been used to target the African nation of Liberia over the past week through a series of short attacks, temporarily taking the country offline . IT security researcher Kevin Beaumont wrote on Thursday (3 November) that these were distributed denial of service (DDoS) attacks. They harnessed a network of compromised computers to create a Mirai botnet, which was designed to flood its target with fake traffic and cripple its servers.'" READ MORE

Source: The Guardian

Date: 4 Nov 2016

How to mitigate impact of cybercrime in Nigeria

"Experts have recommended more proactive measures to mitigate the increasing menace of cybercrime in Nigeria. While the country is said to be loosing about N127 billion yearly to the menace, globally Nigerians are said to be responsible for $9.3 billion share cost of the crime. […] While it has been established that it usually takes 146 days before successful breach is detected by affected organisation, the Chief Information Security Officer, Nigeria Stock Exchange (NSE), Favour Femi-Oyewole, said to successfully tackle cyber security related issues, organisations should focus on developing 'human firewalls.'" READ MORE

Source: Htxt Africa

Date: 14 Nov 2016

Adult website network hacked, 400 million accounts compromised

"Websites belonging to the Friend Finder Network Inc company have been hacked exposing the details of over 400 million accounts. The websites on the network include Adult Friend Finder, Penthouse and iCams among others and represents the largest breach since MySpace revealed it was hacked, earlier this year. The hack – which LeakedSource is calling the biggest of 2016 – was reportedly executed via a Local File Inclusion exploit, which Adult Friend Finder had been made aware of early in October by way of a security researcher. Perhaps the scariest bit of news from this hack is that according to LeakedSource if you thought the Friend Finder Network had deleted your information when you deleted your account, think again." READ MORE

Source: Prachathai

Date: 8 Nov 2016

Thai military teaches staff how to hack computers

"After launching a monitoring centre to suppress online lèse majesté content, the Thai Army has developed intensive courses for its staff that cover basic hacking skills and cyber security. On 8 November 2016, the Royal Thai Army published its cyber security course schedule. The courses aim to train staff at the Army Cyber Centre, established a week earlier to suppress online lèse majesté content, in modern cyber threats and how to prevent them." READ MORE

Latest reports

- Les visages de la lutte contre la cybercriminalité, 3 November 2016
- Court of Justice of the European Union, Pour la CJUE, les IP dynamiques sont aussi des dnnées personelles, Sentence of 19 October 2016

- Eurojust, Cybercrime, encryption, obtaining evidence from the "cloud": report on Eurojust Strategic Seminar "Keys to Cyberspace", published on 4 November 2016
- ENISA, National Cyber Security Strategies Good Practice Guide, 14 November 2016
- UK Government, National Cyber Security Strategy 2016-2021, 1 November 2016
- PaloAlto, Silverterrier: The Next Evolution in Nigerian Cybercrime, 3 November 2016
- SAP, Cyber Threat Intelligence report - November 2016, 8 November 2016
- Delta Risk, State of cybercrime 2016, November 2016

Upcoming events

- 16 – 18 November 2016, Strasbourg, France (Council of Europe) – Participation in the OCTOPUS Conference EAP II, EAP III, GLACY+, iPROCEEDS;
- 21 – 22 November 2016, Kyiv, Ukraine – Seminar on EU Models for International Cooperation, EAP II;
- 24 November 2016, Paris, FRANCE – Study visit of the Moroccan delegation to PHAROS platform on reporting systems, GLACY+;
- 25 November 2016 - Tirana, Albania – Regional workshop for sharing international good practices on reporting mechanisms, iPROCEEDS;
- 1 – 2 December 2016, Turin, ITALY – Participation in UNICRI Cyber Threats Master Class, 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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime