Cybercrime Digest

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

16-30 September 2018

Source: African Union Commission

Date: 20 Sep 2018

The First African Forum on Cybercrime to be hosted by the African Union in Addis Ababa, 16-18 October

"According to recent statistics, the African continent is exhibiting one of the fastest growth rates in Internet penetration worldwide, with digital connectivity that has almost tripled in the last five years. In the same period, both governments and private sector entities in Africa have been experiencing an equally increasing trend of cyber-attacks, in line with what has been recorded also on the global level. […] As a joint organizational effort of African countries, regional and international organizations, the First African Forum on Cybercrime will focus on three major thematic streams: Cybercrime policies and national legislations; International cooperation; Capacity building in Africa. The African Forum on Cybercrime is organized by the African Union Commission and supported by a number of partnering organizations: Council of Europe; the European Union; INTERPOL; UNODC; US DOJ and US State Department; UK Government; the Commonwealth Secretariat." READ MORE Concept Note

Source: INTERPOL

Date: 18 Sep 2018

INTERPOL-Europol conference calls for global response to cybercrime

"Cyber experts from law enforcement, the private sector and academia have gathered in Singapore this week to devise strategies for promoting the global cybersecurity agenda. With cybercriminals using increasingly sophisticated methods and technologies to carry out their illicit activities, the 6th INTERPOL-Europol Cybercrime Conference focused on the most pressing cyberthreats today and in the future, which include attacks against the financial and government sectors, the rise of 'cybercrime as a service', denial of service (DNS) attacks and business e-mail compromise scams. […] Key areas of discussion included developing actionable cyberthreat intelligence, identifying cybercriminals through their online behaviour, defining the role of digital forensics, implementing national and regional legislations to tackle cybercrime, and crisis response planning. " READ MORE

Source: Europol

Date: 28 Sep 2018

15 ways you could be the next victim of cybercrime

"Cybercriminals are adopting creative new techniques to target their victims at an unprecedented pace and are constantly seeking methods to avoid law enforcement detection. To stay ahead of them, law enforcement should target cybercriminals offering "off-the-shelf" cyber-attack services or products to make it more difficult for low-level cybercriminals to carry out high-level attacks. Europol's fifth annual Internet Organised Crime Threat Assessment (IOCTA), presented today at the INTERPOL-Europol Cybercrime Conference in Singapore, offers a unique law enforcement view of the emerging threats and key developments in the field of cybercrime over the last year. But more than that, it describes anticipated future threats and provides recommendations to law enforcement authorities in Europe to adequately deal with these challenges. The report only has one goal in mind: to stop cybercriminals from making you their next victim. " READ MORE

Source: The Guardian

Date: 29 Sep 2018

Facebook says nearly 50m users compromised in huge security breach

"Nearly 50m Facebook accounts were compromised by an attack that gave hackers the ability to take over users' accounts, Facebook revealed on Friday. The breach was discovered by Facebook engineers on Tuesday 25 September, the company said, and patched on Thursday. Users whose accounts were affected will be notified by Facebook. Those users will be logged out of their accounts and required to log back in. […] The security breach is believed to be the largest in Facebook's history and is particularly severe because the attackers stole "access tokens", a kind of security key that allows users to stay logged into Facebook over multiple browsing sessions without entering their password every time." READ MORE

RELATED ARTICLES
Facebook, Security Update, 28 Sep 2018

Source: Balkan Insight

Date: 28 Sep 2018

Serbia tightens cyber security as Internet crime rises

"Serbia's government plans to strengthen the country's cyber-security and the capacity of the police and military to prevent hacking attacks amid a marked rise last year in hi-tech crime. According to the Cybercrime Strategy, Serbia will establish several units within the police, military and customs to fight online crimes. "The strategy is a continuation and expansion of activities aimed at strengthening the efficiency of all entities in the field of suppression of high-tech crime in Serbia," the Strategy, obtained by BIRN, reads. The document, which covers the period between 2019 and 2023, says that by 2020, Serbia will form anti-cybercrime units within the intelligence agency, the BIA, Military Police and Customs Bureau, and also employ more people in existing units with the police. It also added that Serbia will purchase new IT equipment but also specialised software for the police and prosecution, for which about 100,000 euros has been allocated. It states that Serbia will also adopt operational procedures to collect and provide electronic evidence. Civil servants will participate in training, which will be also held for parents, in schools, in the media, and for bank clients, focusing also on child pornography and internet security. " READ MORE

Source: U.S. Department of Defense

Date: 20 Sep 2018

White House Releases First National Cyber Strategy in 15 Years

"The first new National Cyber Strategy in 15 years is built on four pillars: protecting the American people, the homeland and the American way of life; promoting American prosperity; preserving peace through strength; and advancing American influence. "We cannot ignore the costs of malicious cyber activity — economic or otherwise — directed at America's government, businesses and private individuals," President Donald J. Trump said in a statement yesterday announcing the new strategy. "Guided by this [strategy], the federal government will be better equipped to protect the American people, the American homeland, and the American way of life. "Through it," he continued, "we will accomplish critical security objectives while supporting American prosperity, preserving peace through strength and advancing American influence. Informed by the strategy's guidance, federal departments and agencies will more effectively execute their missions to make America cyber secure." READ MORE

Source: Daily FT

Date: 21 Sep 2018

Sri Lanka, National Cyber Security Policy in the offing

"A report titled 'Information and Cyber Security Strategy of Sri Lanka 2018-2023' by the Sri Lanka Computer Emergency Readiness Team | Coordination Centre (Sri Lanka CERT|CC) states, "As the complexity of the cyber security ecosystem increases, the government of Sri Lanka recognises the necessity of introducing a National Information and Cyber Security Strategy to cope with emerging threats." The proposed strategy, which is going to be implemented over a period of five years (2018-2023), will be a high-level top-down approach to information and cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe. "To further strengthen our regulatory framework to effectively battle emerging cybercrimes, gaps in the existing policies and laws will be identified, and new legislation, policies, and standards will be drafted and implemented." […] A National Information and Cyber Security Agency (NICSA) will also be established. "The Agency will be responsible for overseeing the implementation of the cyber security strategy, setting national polices, facilitating the protection of critical national infrastructure, educating citizens, building a pioneering technology competent workforce, and promoting industry development," further states the report. " READ MORE

Source: Cooperativa

Date: 22 Sep 2018

Chile: Gobierno creará la figura del "coordinador nacional de ciberseguridad"

"En el marco del proyecto contra los delitos informáticos que presentará los primeros días de octubre, el Gobierno creará una figura que se encargará de coordinar a distintos ministerios en pos del cumplimiento de las normas. Así lo anunciaron el subsecretario del Interior, Rodrigo Ubilla, y delegado presidencial para temas de ciberseguridad, Jorge Atton, quienes adelantaron detalles de la iniciativa en una entrevista conjunta en El Mercurio. Ubilla explicó que se "establecerá una etapa intermedia, se que llama 'gobernanza provisoria', para evaluar el funcionamiento de la estructura antes de impulsar el proyecto de infraestructura crítica" […] Atton resaltó que el proyecto contemplará la tipificación de delitos informático de acueredo con los establecido en el Convenio de Budapest, que entró en vigor en 2004 en el mundo y fue ratificado por Chile en 2017." READ MORE

Source: Caribbean News

Date: 26 Sep 2018

Nine out of ten banks in Latin America and the Caribbean suffered cyber incidents during the last year, says OAS

"On Tuesday, the Organization of American States (OAS) presented a report on the "State of Cybersecurity in the Banking Sector in Latin America and the Caribbean", which includes an analysis of the past year in the banking sector and online banking users in aspects related to cybersecurity. The main findings of the report are: (i) At least nine out of ten banking entities suffered cyber incidents during the last year; (ii) 37 percent of the banks in the region were victims of successful attacks; (iii) 39 percent of the incidents were not reported, in the case of the largest banking entities this number goes down to 19 percent; (iv) Six out of ten users, who do not use digital banking services, don't trust the security of bank transactions." READ MORE

Source: The Straits Times

Date: 20 Sep 2018

Asean framework on cyber security in the works

"Asean will work towards a rules-based international framework on cyber security, and Singapore will continue to lead efforts to bolster the region's cyber defences, said Minister for Communications and Information S. Iswaran. Chairing the Asean Ministerial Conference on Cybersecurity yesterday, Mr Iswaran, who is also Minister-in-charge of Cyber Security, said all 10 Asean states agree that this rules-based approach would give the region confidence to better deal with cyberthreats. Recognising that a rules-based cyberspace would allow for economic progress and better living standards, the AMCC also agreed to subscribe in principle to 11 voluntary norms recommended in the 2015 Report of the UN Group of Experts on Developments in the Field of Information and Telecommunications in the context of International Security." READ MORE

Source: ZDNet

Date: 27 Sep 2018

Port of San Diego suffers cyber-attack, second port in a week after Barcelona

"Two major international ports fell victim to cyber-attacks within the span of a week, putting the shipping industry on alert for a possible threat actor targeting the entire sector. The first to fall was the Port of Barcelona, Spain, on September 20, last week. The second attack was reported yesterday, September 25, by the Port of San Diego, in the United States. None of the two port authorities revealed any details about the nature of the cyber-attacks, leaving security experts to speculate about possible causes. The cyber-attack on the Port of Barcelona did not affect ship movements in and out of the harbor, and a local newspaper reported that it impacted only land operations, such as loading or unloading of boats, although the Port denied there was a serious disruption to customers." READ MORE

Source: CNN

Date: 26 Sep 2018

Uber to pay record $148 million over 2016 data breach

"The settlement with attorneys general for all 50 states and Washington, DC, will be split among the states. It's the largest ever multi-state data breach settlement, according to the New York attorney general. The investigation was called to look into allegations that the ride-share company violated state-level notification laws by intentionally withholding that hackers stole the personal information of 57 million users in 2016. The breach wasn't disclosed until late 2017, when Uber revealed that it paid the hackers $100,000 to destroy the data. " READ MORE

Source: Reuters

Date: 23 Sep 2018

China shuts thousands of websites in clean-up campaign

"China has shut down more than 4,000 websites and online accounts in a three-month campaign against "harmful" online information, the official Xinhua news agency said on Saturday, citing the country's illegal publication watchdog. China keeps the internet under tight control and has been cracking down on a range of illegal online activities including pornography, gambling, religious proselytizing and even "spreading rumors". […] Authorities announced last week that they had busted a live-streaming pornography platform hosted in Cambodia and said to have more than 3.5 million registered users." READ MORE

Source: Avast

Date: 27 Sep 2018

New, sophisticated IoT botnet targets a wide range of devices

"Over the past week, we have been observing a new malware strain, which we call Torii, that differs from Mirai and other botnets we know of, particularly in the advanced techniques it uses. Unlike the aforementioned IoT botnets, this one tries to be more stealthy and persistent once the device is compromised, and it does not (yet) do the usual stuff a botnet does like DDOS, attacking all the devices connected to the internet, or, of course, mining cryptocurrencies. Instead, it comes with a quite rich set of features for exfiltration of (sensitive) information, modular architecture capable of fetching and executing other commands and executables and all of it via multiple layers of encrypted communication. Furthermore, Torii can infect a wide range of devices and it provides support for a wide range of target architectures, including MIPS, ARM, x86, x64, PowerPC, SuperH, and others. Definitely, one of the largest sets we've seen so far. As we've been digging into this strain, we've found indications that this operation has been running since December 2017, maybe even longer." READ MORE

Latest reports

- European Commission, Speech by Commissioner Avramopoulos at the ministerial conference on high-tech crime and information security "Connect securely", 20 Sep 2018
- Europol, Internet Organized Crime Threat Assessment 2018, 18 Sep 2018
- ENISA, National Cyber Security Strategies Evaluation Tool, 18 Sep 2018
- White House, National Cyber Strategy of the United States, September 2018
- OAS, State of Cybersecurity in the Banking Sector in Latin America and the Caribbean, 26 Sep 2018
- Fortinet, 2018 Security Implications of Digital Transformation, August 2018

Upcoming events

- 1-4 October, Bihać, Bosnia and Herzegovina – Pilot training introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors, iPROCEEDS
- 1-5 October, Yerevan, Armenia – Joint training of 24/7 points of contact and other SPCs from investigative agencies with the use of ECTEG materials, Cybercrime@EAP 2018
- 01-05 October, Rabat, Morocco – Advanced judicial training on cybercrime and electronic evidence, CyberSouth
- 2-5 October, Nairobi, Kenya – Data protection legislation workshop, Cybercrime@Octopus
- 4 – 5 October, Zagreb, Croatia – Regional Forum on Online Fraud in South-eastern Europe in cooperation with the Judicial Academy of Croatia, iPROCEEDS
- 08-09 October, Amman, Jordan – Awareness raising meeting on the Budapest Convention and its instruments, CyberSouth
- 8-11 October, San José, Costa Rica – Advisory mission on harmonization of legislation on cybercrime and electronic evidence and workshop on cybercrime and cyber security policies and strategies, GLACY+
- 9-10 October, Minsk, Belarus – National Cybercrime Cooperation Forum with participation of law enforcement and Internet industry / contribute to OSCE Conference, Cybercrime@EAP 2018
- 11-12 October, Minsk Belarus – Table top exercise on interagency cooperation in the context of international cooperation on cybercrime and electronic evidence, Cybercrime@EAP 2018
- 12 October, Bucharest, Romania – Planning event for the CEAP IV project, Cybercrime@EAP 2018

- 15-16 October, Tbilisi, Georgia – Table top exercise on interagency cooperation in the context of international cooperation on cybercrime and electronic evidence, Cybercrime@EAP 2018
- 15-19 October, Nairobi, Kenya – Cybercrime Investigation Training for African Region, GLACY+
- 15-19 October, Ankara, Turkey – ECTEG regional training on Malware Investigations in cooperation with the Department of Cybercrime, Turkish National Police, iPROCEEDS
- 16-18 October, Addis Ababa, Ethiopia – African Forum on Cybercrime: Policies and Legislation, International Cooperation and Capacity Building, GLACY+ /Cybercrime@Octopus /CyberSouth

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