Cybercrime Digest

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

16-31 December 2018

Source: Ministère de l'Enseignement Supérieur et de la Recherche Scientifique, des Technologies de l'Information et de la Communication, République Islamique de Mauritanie

Date: 17 Dec 2018

Atelier de préparation du processus d'adhésion de la Mauritanie à la Convention de Budapest sur la Cybercriminalité

"Les travaux de l'atelier de préparation du processus d'adhésion de la Mauritanie à la Convention de Budapest sur la Cybercriminalité, organisé par le ministère de l'enseignement supérieur, de la recherche scientifique et des technologies de l'information et de la communication en collaboration avec l'Union Européenne, ont débuté lundi matin à Nouakchott. La rencontre de trois jours a pour objectif de développer et de renforcer la législation nationale pays en matière de cybercriminalité et des preuves électroniques, de tirer profit de cette convention, en respectant les droits de l'homme et l'état de droit, et de procéder à une évaluation des besoins du pays en matière de renforcement des capacités de lutte contre la cybercriminalité et d'utilisation appropriée des preuves électroniques." READ MORE

Source: Council of Europe

Date: 21 Dec 2018

GLACY+: ECTEG course on Internet and darkweb Investigation in Senegal

"In the framework of the GLACY+ Project, the ECTEG course on Internet and darkweb Investigation was delivered to the law enforcement officers in Senegal during 17-21 December 2018 by INTERPOL in its capacity as the implementing partner of the project. The goal of the training was to provide the officers with competencies to perform Internet investigation with enhanced knowledge in the relevant technologies." READ MORE

Source: ASEAN Today

Date: 21 Dec 2018

The ASEAN governments exploiting cybersecurity threats to expand authoritarian powers

"Three-quarters of ASEAN's population is expected to have internet access by 2020 – a sharp jump from the 260 million users in 2017 to 480 million in 2020. As access has expanded, Southeast Asian states have seen a series of security breaches that violate the privacy and security of their citizens. […] As internet access has expanded in Southeast Asia, many of the region's governments have responded with digital authoritarianism, by restricting free use of the web and using new and existing laws to punish dissent. […] Myanmar has seen expanded use of an existing measure, clause 66(d) of the 2013 Telecommunications Law, to prosecute journalists and activists for posting anything online that the state deems to be "defamatory." […] In Thailand the junta has proposed creating a new National Cybersecurity Committee (NCSC), with the power to surveil internet traffic, confiscate computers as they see fit and order sites to remove content that they find objectionable. […] Cambodia is pursuing similar measures, with the announcement of a new National Anti-Cybercrime Committee that will have the power to arrest citizens for posting content online. […] In Vietnam, a new cybersecurity law will require all companies operating in the country to store data on servers inside the country, and therefore be subject to Vietnamese law." READ MORE

Source: Reuters

Date: 17 Dec 2018

Maroc, la DGSN dresse son bilan sur la Cybercriminalité

"Les crimes de cybercriminalité ont connu une augmentation de 33% en 2018 avec 1.091 affaires traitées contre 765 en 2017, fait état la DGSN dans un communiqué rendu public mardi sur le bilan de ses réalisations au titre de l'année 2018 et son programme d'action pour 2019. Les services de la Direction générale de la sûreté nationale (DGSN) précisent qu'un tiers de ces affaires a été détecté grâce au système de veille adopté par la direction de police judiciaire, selon la même source. Quant au nombre des affaires de chantage sexuel via internet, il a atteint 435, ayant abouti à l'interpellation de 267 escrocs, pour un total de 435 victimes, dont 125 étrangers." READ MORE

Source: U.S. Department of Justice

Date: 21 Dec 2018

Two Chinese hackers associated with the Ministry of State Security charged with computer intrusion in U.S.

"The unsealing of an indictment charging Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller; and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, both nationals of the People's Republic of China (China), with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft was announced today. […] Zhu and Zhang were members of a hacking group operating in China known within the cyber security community as Advanced Persistent Threat 10 (the APT10 Group). […] Through their involvement with the APT10 Group, from at least in or about 2006 up to and including in or about 2018, Zhu and Zhang conducted global campaigns of computer intrusions targeting, among other data, intellectual property and confidential business and technological information at managed service providers (MSPs), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, more than 45 technology companies in at least a dozen U.S. states, and U.S. government agencies." READ MORE

RELATED ARTICLES

Reuters, German security office warned German firms about Chinese hacking, 19 Dec 2018

Source: HackRead

Date: 20 Dec 2018

Facebook bug exposed private photos of 6.8M users to third-party developers

"Facebook has announced that a bug in its Photo API exposed private photos of over 6.8 million users to third-party app developers. The breach took place from September 13 to September 25, 2018, which means for 12 days straight some developers could view your personal and private photos without any restriction and without your consent. The company believes that up to 1,500 apps built by 876 developers had access to user's photos. This included photos uploaded by users on their Facebook Stories and Marketplace. Unsurprising, this also included photos that users uploaded to Facebook but decided not to post. It is noteworthy that Facebook saves a copy of everything a user does on the timeline box including unpublished statuses and photos." READ MORE

Source: Reuters

Date: 17 Dec 2018

Russia used social media for widespread meddling in U.S. politics: reports

"Russian interference in the 2016 U.S. presidential election on social media was more widespread than previously thought and included attempts to divide Americans by race and extreme ideology, said reports by private experts released on Monday by U.S. senators from both parties. The Russian government's Internet Research Agency tried to manipulate U.S. politics, said the reports, one by social media analysts New Knowledge and the other by an Oxford University team working with analytical firm Graphika. The twin reports largely verified earlier findings by U.S. intelligence agencies, but offered much more detail about Russian activity going back years that continues even now, said the reports and senior lawmakers." READ MORE

Source: Engadget

Date: 20 Dec 2018

Twitter and Facebook target fake accounts ahead of Bangladesh election

"Both Facebook and Twitter have removed a handful of accounts ahead of Bangladesh's general election, citing coordinated manipulation and inauthentic behavior as their reasons. Facebook took down nine Pages and six accounts while Twitter suspended 15 accounts. Twitter said most of the accounts it removed had fewer than 50 followers and Facebook reported that around 11,900 people followed at least one of the Pages it took down. […] Facebook determined that the accounts in question were designed to resemble those of legitimate news outlets, such as BBC's Bangla news service and Bangladesh's bdnews24.com, but were focused on posting anti-opposition content. "This kind of behavior is not allowed on Facebook under our misrepresentation policy because we don't want people or organizations creating networks of accounts to mislead others about who they are, or what they're doing," Facebook's cybersecurity policy head Nathaniel Gleicher wrote in a blog post. Over the past two years, Facebook has removed fake accounts head of elections in France, Germany, Brazil, Mexico and the US. Twitter also recently detailed the efforts it has made to secure elections around the world." READ MORE

Source: Albawaba

Date: 18 Dec 2018

Lebanon Seeks to Create Agency to Fight Cyber Crime

"A committee tasked with creating Lebanon's cybersecurity strategy expects to present its recommendations - including the creation of a national cybersecurity agency - to Parliament in five months, according to National ICT Strategy Coordinator Lina Oueidat. Oueidat said among the committee's recommendations was the creation of a "National Agency for Information Service Security" that would be responsible for addressing cybercrime. The committee, comprised of representatives from the government's key ministries, intelligence and military arms and the private sector, was formed in November at the behest of Prime Minister-designate Saad Hariri to institutionalize cybersecurity in the Lebanese state. […] According to Jerome Ribault Gaillard, a member of the EU delegation in Lebanon, the country needs to take urgent action to enhance its cybersecurity, as it is highly vulnerable to cyberattacks. […] "You need better legislation in your Parliament - you need a better understanding of who is doing what in case of an attack," Gaillard said, adding that the EU supported Lebanon in this process." READ MORE

Source: Viet Nam news

Date: 19 Dec 2018

Viet Nam faces high risk of online child sexual exploitation

"Việt Nam is one of the countries with the fastest internet development rate and highest number of social media users in the world. Pedophiles have been taking advantage of social media and online chat forums to approach their victims and make sexual advances, said Dr Lại Kiên Cường, deputy head of the high-tech crime unit of the People's Police Academy. Police and prosecutors often struggle to find evidence of sexual harassment in these cases since incriminating conversations are in a digital form and are easily erased, he said. Around 1,500 to 1,800 child sexual exploitation cases are reported and prosecuted in Việt Nam each year, but a lot more remained undiscovered due to fear of shame from the victims and their families." READ MORE

Source: Bangkok Post

Date: 19 Dec 2018

Thailand, Cyberbill to be tabled next week

"The cybersecurity bill, which critics say could give ways for authorities to violate citizens' rights, is expected to be tabled before the cabinet meeting next week. Paiboon Amonpinyokeat, a member of the national cyber preparation committee, said the bill has been redressed to standardise the appeal process with the court. […] The bill, he said, will usher in three main structures -- an administrative unit, a security surveillance panel, chaired by a deputy prime minister in charge of security affairs, as well as a committee dealing with economic measures. "It is likely to be forwarded to the cabinet next week," said Mr Paiboon. The bill calls for the establishment of a Cyber Security Agency, which critics say would be given too much power. It allows for the seizure of computer servers or other assets without a court order. Department of Special Investigation (DSI) chief Paisit Wongmuang said the bill would also lead to the establishment of a centre to receive cyber violations complaints." READ MORE

Source: InfoArmor

Date: 14 Dec 2018

Identification numbers of 120 million Brazilians exposed online

"In March of 2018, the InfoArmor Advanced Threat Intelligence team discovered an open http server during regular internet scanning for compromised machines, building of IP reputations, and threat actor activity. The misconfigured, publicly accessible server contained 120 million unique Cadastro de Pessoas Físicas (CPFs). CPFs are an identification number issued by the Brazilian Federal Reserve to Brazilian citizens and tax-paying resident aliens, and each exposed CFP linked to an individual's banks, loans, repayments, credit and debit history, voting history, full name, emails, residential addresses, phone numbers, date of birth, family contacts, employment, voting registration numbers, contract numbers, and contract amounts." READ MORE

Source: Bulawayo 24 News

Date: 18 Dec 2018

Zimbabwe, Cabinet approves Cyber Crime bill

"Cabinet has approved the principles for Cyber Protection, Data Protection and Electronic Transaction Bill, the Minister of Information Monica Mutsvangwa has revealed. Addressing a post cabinet media briefing Mutsvangwa said the Bill will among other things, harmonise computer crime laws to the SADC Model laws, the admissibility of electronic evidence, regulation of access to information, protection of privacy and processing of personal data by automated means." READ MORE

Source: The Star

Date: 20 Dec 2018

Kenya, cyber threats now at worrying levels

"Nearly all cyber threats and attacks detected between July and September went unresolved, the latest communication sector statistics show. Communications Authority's first quarter report for 2018/19 shows the National Cybersecurity Centre detected 3.82 million cyber threats, a rise from 3.46 million reported between April and June. The threat exposes many Kenyan companies, institutions and co-operative societies to the risk losing billions of shillings. Within the review period, the banking sector remained the most targeted industry followed by government institutions. The CA report indicates that 0.17 per cent (6,384) of the total threats were determined as critical, validated and escalated for action. This was an increase from the previous quarter, where 2,613 cases were validated and escalated." READ MORE

Source: Fiji Sun Online

Date: 16 Dec 2018

Financial Institution And Members Of The Public Rise In Email Compromise And Email Spoofing Cases In Fiji

"The Fiji FIU would like to advise commercial banks, financial in-stitutions, businesses and members of the public to exercise caution when handling email payment instructions for import trade transactions and large value personal out-bound foreign remittance transactions. The Fiji FIU has noticed a continuous rise in cases of individuals and businesses falling victim to email compromise and spoofing scams. Since 2014, 39 businesses and individuals have lost funds totaling $5million in foreign remittance transactions to cybercriminals through email compromise scams. Only $169,000 was recovered." READ MORE

Latest reports

- Council of Europe, Snapshot of the Cybercrime@EAP 2018 results, 17 Dec 2018
- Ministry of Technology, Communication and Innovation of Mauritius, Digital Mauritius 2030 Strategic Plan, December 2018
- IEEE Spectrum, The Biggest IT Failures of 2018, 27 Dec 2018
- Computer Weekly, Top 10 cyber crime stories of 2018, 21 Dec 2018
- IBM X-Force, Security Predictions for the 2019 Cybercrime Threat Landscape, 20 Dec 2018
- KnowTechie, Cyber Security in 2019 – What are the predictions, 31 Dec 2018

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