Cybercrime Digest

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

1-15 January 2019

Source: Reuters

Date: 4 Jan 2019

German politicians' data published online in massive breach

"Personal data and documents from hundreds of German politicians and public figures including Chancellor Angela Merkel have been published online in what appears to be one of Germany's most far-reaching data breaches. A preliminary analysis showed the data had been obtained through "wrongful use of log-in information for cloud services, email accounts or social networks", Interior Minister Horst Seehofer said in a statement late on Friday. He said there was no evidence that the computer systems of the German lower house of parliament or the government had been compromised, but provided no further details. The ministry said it remained unclear if the breach, which triggered an emergency meeting of the BSI national cyber defense agency, was the result of a hack or a leak." READ MORE

Source: The Irish Times

Date: 17 Jan 2019

Ireland, Government fails to ratify child protection conventions

"The Government has failed to ratify two international conventions on child protection four years after the special rapporteur called for the State to do so and more than a decade after they were signed. Fianna Fáil justice spokesman Jim O'Callaghan said the State signed the Budapest Convention on cybercrime in 2001 and the Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse in 2007. Minister for Justice Charlie Flanagan said much work had been done on the conventions and that "the vast majority of the provisions in the cybercrime convention are provided for in Irish law". And the Government legislative programme makes provision for the drafting of a new cybercrime Bill to give effect to those remaining provisions of the convention, not already provided for in domestic law. […] The special rapporteur on the protection of children Dr Geoffrey Shannon "expressly" brought the issue to the attention of the Government in 2014 and said that in order to ensure the highest standards of protection for children and the highest level of international co-operation in this area "it is imperative that both conventions are ratified"." READ MORE

Source: Nasdaq

Date: 19 Jan 2019

Turkey sentences detained judge who won human rights award to 10 years

"A Turkish court sentenced a judge who previously won an award for human rights to 10 years in prison over links to the network Ankara says orchestrated an attempted coup in 2016, the state-owned Anadolu news agency said on Friday. Murat Arslan, who has been detained for 22 months, was convicted of membership in an armed terrorist organisation, after prosecutors charged him with use of the encrypted messaging app ByLock. Arslan has denied the charges and said any evidence that he had used the app was "fabricated". […] The Council of Europe human rights body in 2017 gave Arslan, who was detained at the time, the Vaclav Havel Human Rights Prize, a decision that prompted Turkey to say it would cut back its funding to the body." READ MORE

Source: ThreatPost

Date: 17 Jan 2019

Cyber-Jackpot: 773M Credentials Dumped on the Dark Web

"A database of breached emails totaling 773 million unique addresses has turned up on a popular underground hacking forum, giving cybercriminals one of the largest jackpots ever seen when it comes to account-compromise efforts. Troy Hunt was first alerted to the cache, which totals 87GB of data, after it was seen being hosted on the MEGA cloud service. The data was organized into 12,000 separate files under a root folder called "Collection #1," which gives the trove its name. Soon after that, the whole shebang turned up on the cyber-underground. In examining the data, Hunt found that there are 1.16 billion unique combinations of email addresses and passwords listed. And after deduping and cleaning up the database, Hunt was left with about 773 million unique email addresses […]. The consequences of account access can range from very productive phishing, as criminals can automatically send malicious e-mails to a victim's list of contacts, to targeted attacks designed to steal victims' entire digital identity or money or to compromise their social media network data" READ MORE

Source: Daily Mail

Date: 16 Jan 2019

Portuguese computer hacker named as Football Leaks arrested in Hungary

"A Portuguese hacker named as the cyber criminal behind Football Leaks has been arrested in Hungary. The 30-year-old, who media in Lisbon are claiming is a university dropout called Rui Pinto, was held following a lengthy investigation by Portugal's Policia Judiciaria. Pinto has been forced to deny he is the mystery individual who revealed the rape claim against Ronaldo, alleged breaches of financial fair play rules by Manchester City and the infamous Beckham emails in which he allegedly branded the honours committee 'unappreciative c#### for missing out on a knighthood.' […] Portugal's Policia Judiciaria police confirmed the arrest of an unnamed 30-year-old in a press release. A spokesman said he was held on a European Arrest Warrant on suspicion of crimes of attempted extortion and theft of trade secrets following an investigation involving a national Portuguese police cybercrime unit." READ MORE

Source: National Crime Agency UK

Date: 13 Jan 2019

International hacker-for-hire jailed for cyber attacks on Liberian telecommunications provider

"A British cyber criminal has been sentenced to two years and eight months for conducting attacks that disrupted a Liberian telecommunications provider, resulting in losses estimated at tens of millions of US dollars. Daniel Kaye, from Egham, Surrey, pleaded guilty in December 2018 to creating and using a botnet and possessing criminal property. He was jailed today following an investigation led by the NCA's National Cyber Crime Unit. Kaye, who was living in Peyia, Cyprus, began carrying out intermittent DDoS attacks on the Liberian telecommunications provider Lonestar MTN in October 2015 using rented botnets and stressors. The 30-year-old expert hacker was hired by a senior official at Cellcom, a rival Liberian network provider, and paid a monthly retainer. From September 2016, Kaye used his own Mirai botnet, made up of a network of infected Dahua security cameras, to carry out consistent attacks on Lonestar. In November 2016, the traffic from Kaye's botnet was so high in volume that it disabled internet access across Liberia." READ MORE

Source: Wired

Date: 9 Jan 2019

A growing frontier for Terrorist Groups: unsuspecting Chat Apps

"ISIS has effectively exploited the power of technology to fuel its rise around the globe, from streaming and file-sharing platforms to messenger applications and social media services. Many tech companies have responded in turn, strengthening their oversight and security measures. But while major platforms like Facebook, Twitter, YouTube, and Telegram are becoming increasingly inhospitable to ISIS, the group's reach is growing on lesser-known messenger apps designed for businesses and gamers. In the aftermath of major territory losses in Iraq and Syria, ISIS is reconfiguring how it uses technology to drive its recruitment and coordination efforts. ISIS uses the encrypted messenger platform Telegram as its primary app for media releases. In seeking new venues to disseminate its content, the terrorist group has made repeated attempts to set up web pages and blogs on services like Tumblr and WordPress. Such platforms are fitting places for ISIS propaganda, where content can be transferred from Telegram into organized, easily accessible layouts." READ MORE

Source: Reuters

Date: 13 Jan 2019

German antitrust watchdog to act against Facebook

"Germany's antitrust watchdog plans to order Facebook to stop gathering some user data, a newspaper reported on Sunday. The Federal Cartel Office, which has been investigating Facebook since 2015, has already found that the social media giant abused its market dominance to gather data on people without their knowledge or consent. The Bild am Sonntag newspaper said the watchdog will present the U.S. company with its ruling on what action it needs to take in the next few weeks." READ MORE

Source: Diario Constitucional

Date: 8 Jan 2019

Chile, Comisión de Seguridad Pública del Senado reabre debate sul proyecto de ciberseguridad

"El proyecto iniciado en mensaje, tiene como objetivo central derogar la ley N° 19.223, con el objeto de establecer una ley especial que contenga de manera integral las nuevas formas delictivas surgidas a partir del desarrollo de la informática. Para ello plantea una serie de cambios como: [1] Modificar el tratamiento que se entrega actualmente al sabotaje y espionaje informático, adecuándolos a las figuras penales reconocidas en el Convenio de Budapest, a saber: acceso ilícito a todo o parte de un sistema informático, ataque a la integridad del sistema y de los datos informáticos. [2] Agregar el delito de interceptación o interferencia indebida y maliciosa de las transmisiones no públicas entre sistemas informáticos, y la captación ilícita de datos transportados mediante emisiones electromagnéticas de sistemas informáticos, en concordancia con el delito de interceptación ilícita contenido en el Convenio de Budapest. [3] Incorporar el delito de falsificación informática, contenido en el Convenio de Budapest, que comprende la maliciosa introducción, alteración, borrado o supresión que genere datos no auténticos con el propósito de hacerlos pasar como "auténticos o fiables" por un tercero. [4] Incluir como delito, la defraudación a otro utilizando la información contenida en un sistema informático al que se hubieren introducido ilegítimamente datos informáticos o aprovechándose de la alteración, daño o supresión de documentos electrónicos o de datos transmitidos o contenidos en un sistema informático." READ MORE

Source: CNET

Date: 9 Jan 2019

Facebook in violation of new cybersecurity law, says Vietnam

"The social network has infringed on a new cybersecurity law in the country by letting users post content it deemed illegal on its platform, state media reported Wednesday. Such posts include those containing "slanderous content," "anti-government sentiment" and the defamation of individuals and organisations, it added, citing the Ministry of Information and Communications. Despite repeated emails, Facebook did not remove the offending content and refused to hand over information on "fraudulent accounts" to the authorities. The report comes more than a week after a controversial law came into effect on Jan. 1. The law requires internet companies to keep user data locally, remove offending content from their platforms and provide user data to the government without the need for a warrant. Vietnam's existing rules penalise comments online that contain "propaganda against the state" and "reactionary ideology."." READ MORE

Source: Getting the Deal Through

Date: January 2019

Privacy and cyber security in Peru

"Peru does not have a Cybersecurity Law in force; nevertheless, there are several pieces of legislation that apply to this field. […] In 2000, Law No. 27,309 added cybercrimes to the Penal Code. In 2013, Law No. 30,096 (the Cybercrimes Law) replaced most of the Penal Code provisions, and finally Law No. 30,171 amended Law No. 30,096. Before the creation of legislation targeting these specific types of crime, most of the incidents investigated were processed as new forms of scams. Nowadays, unlawful access to systems by breaching security measures, unlawful distortion of data, illegal traffic of data and data interception, among other things, are prosecuted as cybercrimes, which are – of course – more serious offences than scams." READ MORE

Source: Open Global Rights

Date: 10 Jan 2019

Restricting cybersecurity, violating human rights: cybercrime laws in MENA region

"For example, the Bahraini "Cybercrime Law", passed in 2014, gives various government organizations, including the Ministry of Interior and the Ministry of Public Information, the capacity to block and censor a wide range of websites. No court order is needed to censor websites that host content deemed a "challenge" to the government, such as any published content that is critical of the Bahraini government, the royal family, or the status quo generally. Similar censorship is found in the Egyptian Cybercrime Law passed in 2018. Under Article 7, any website can be blocked if its content is considered a crime under the law, provided that it poses a threat to national security or jeopardizes the security of the country or its national economy—effectively legalizing the blocking of websites. These laws also facilitate and legalize mass surveillance by the state and foreign governments. For instance, the Egyptian law enables the violation of Egyptians' right to privacy by foreign governments. Article 4 of the law addresses the exchange of data and information between Egypt and foreign countries through the Ministries of Foreign Affairs and International Cooperation within the framework of international, regional, and bilateral agreements or the application of the principle of reciprocity. The article does not include any requirements for the exchange of such information, such as the existence of data protection laws in the requesting country or requirements regarding the scope, duration of retention, or processing of information." READ MORE

Source: The Straits Times

Date: 10 Jan 2019

Manila ex-banker gets jail, $147 million fine over Bangladesh cyber heist

"A Philippine former banker was handed a lengthy jail term and US$109 million (S$147 million) fine on Thursday (Jan 10) in the first conviction over one of the biggest ever cyber heists which saw US$81 million stolen from Bangladesh's central bank. […] The authorities charged that Deguito helped coordinate the transfer of the money, which was taken from Bangladesh's reserves account at the Federal Reserve bank in the United States. […] A North Korean hacker is also wanted by the US on charges that he and a state-sponsored hacking crew masterminded the Bangladesh heist. Only US$15 million of the money was recovered after it landed in the Philippines and was quickly dispersed. Tens of millions of the loot disappeared into Manila's casinos, which were at the time exempt from rules aimed at preventing money laundering." READ MORE

Source: Reuters

Date: 2 Jan 2019

Sudan restricts social media access to counter protest

"Sudanese authorities are blocking access to popular social media platforms used to organize and broadcast nationwide anti-government protests triggered by an economic crisis, internet users say. […] In a country where the state tightly controls traditional media, the internet has become a key information battleground. Of Sudan's 40 million people, some 13 million use the internet and more than 28 million own mobile phones, local media say. […] Users of the three main telecommunications operators in the country said access to Facebook, Twitter and WhatsApp has only been possible through use of a virtual private network (VPN). Though VPNs can bring their own connection problems and some Sudanese are unaware of their existence, activists have used them widely to organize and document the demonstrations." READ MORE

Source: ZD Net

Date: 1 Jan 2019

Explosion in digital evidence coming thanks to IoT and 5G

"5G is expected to be commercialised early this year. This will be a further catalyst for growth in digital evidence. Already, data is being saved through smart home services such as home security and pet monitoring. Drones and autonomous vehicles are producing new video data each day. CCTVs, DVRs, and black boxes in cars among other Internet of Things (IoT) devices are increasingly becoming more sophisticated. There will be an explosion of data, and digital forensics is evolving further to meet that demand, says Jun. "Videos are becoming increasingly high resolution and there are a variety of codecs being developed and uses. In CCTVs, each manufacturer uses different media format to save data. The time it takes to recover and analyze data is increasing; there is a demand for recovery algorithms backed by high-performance hardware," the managing director said. "For investigators, they now have to consider every peripheral device besides the smartphones for evidence. This is a challenge; but it is also a great opportunity." Data saved on IoT devices is also stored via gateways on the cloud; this data is in turn viewed again by consumers usually through their mobile devices. "Anyone of these data intersections can be the subject of forensics; the more routes data takes, the higher the possibility to recover that data"." READ MORE

Latest reports

- Parliamentary Assembly of the Council of Europe (PACE), Committee on Culture, Science, Education and Media, Internet governance and human rights, 4 Jan 2019
- CircleID, Internet Governance Outlook 2019: Innovative Multilateralism vs. Neo-Nationalistic Unilateralism, 8 Jan 2019
- Thomson Reuters, The Rise of Global State-Attributed Cyberattacks, 2005-2018, January 2019
- WatchGuard Threat Labs, 2019 Security Predictions, January 2019
- Emil Hozan, My Journey into the Dark Web: At Your Service, 9 Jan 2019

Upcoming events

- 14-18 January, Bucharest, Romania – ECTEG E-First Working Group, CyberSouth
- 16-19 January, Beirut, Lebanon – Advanced Judicial Training, CyberSouth
- 21-24 January, Guatemala City – Advisory mission on harmonization of legislation on cybercrime and electronic evidence, GLACY+
- 21-24 January, Jakarta, Indonesia – Introductory Judicial Training on Cybercrime and Electronic Evidence for Indonesian judges, magistrates and prosecutors, delivered by Filipino trainers, GLACY+
- 23-25 January, Beirut, Lebanon – Regional workshop on the judicial training strategy, CyberSouth
- 28 January – 1 February, Abuja, Nigeria - Introductory ToT on Cybercrime and Electronic Evidence for judges, prosecutors and lawyers and adaptation of materials to the local context, GLACY+
- 29 January, Tirana, Albania – Meeting to support existing public/private initiatives or establish such mechanisms at domestic level, iPROCEEDS

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime