Cybercrime Digest

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

1-15 May 2019

Source: Council of Europe

Date: 2 May 2019

Le Conseil de l'Europe a 70 ans : temps forts et réalisations

"Le Conseil de l'Europe a créé un espace juridique commun sans peine de mort pour 830 millions de personnes dans 47 pays. […] Nous avons élaboré plus de 200 traités internationaux juridiquement contraignants pour contribuer à protéger les gens de menaces spécifiques telles que la torture, la violence et les abus sexuels, ainsi que pour renforcer les normes internationales sur des questions comme la cybercriminalité et la protection des données. […] Les 47 pays du Conseil de l'Europe ont signé la Convention de Lanzarote sur la protection des enfants contre l'exploitation et les abus sexuels – 44 ratifiée. 54 pays dans le monde sont maintenant couverts par la convention du Conseil de l'Europe sur la protection des données et 63 pays – dont les États-Unis, l'Australie et le Japon – par la convention sur la cybercriminalité." READ MORE

RELATED ARTICLES

Council of Europe, The Council of Europe at 70: Milestones and achievements, 2 May 2019

Source: Reuters

Date: 10 May 2019

G7 countries to simulate cross-border cyber attack next month: France

"Leading Western industrial powers will for the first time jointly simulate a major cross-border cyber security attack on the financial sector next month, French officials said on Friday. The exercise, organized by the French central bank under France's presidency of the Group of Seven nations (G7), will be based on the scenario of a technical component widely used in the financial sector becoming infected with malware, said Nathalie Aufauvre, the Bank of France's director general for financial stability. Institutions such as the European Central Bank and the Bank of England have already conducted such tests, but the June exercise will be the first across borders at the G7 level, Aufauvre told a cyber security conference at the bank." READ MORE

RELATED ARTICLES

G7, Foreign Ministers Meeting Communiqué, 5-6 Apr 2019

Source: FRA

Date: 14 May 2019

FRA to host expert meeting on cybercrime and fundamental rights

"The agency will host, in cooperation with the Council of Europe, the second expert meeting on cybercrime and fundamental rights from 14 to 15 May. FRA has invited experts from relevant European and international stakeholders on the fight against cybercrime. These include the European Commission, the cybercrime division of the Council of Europe, EU agencies such as Europol, Eurojust, and ENISA, the European Judicial Network, the UN Office on Drugs and Crime, the OSCE as well as representatives of national prosecution services." READ MORE

Source: Europol

Date: 16 May 2019

Goznym malware: cybercriminal network dismantled in international operation

"An unprecedented, international law enforcement operation has dismantled a complex, globally operating and organised cybercrime network. The criminal network used GozNym malware in an attempt to steal an estimated $100 million from more than 41 000 victims, primarily businesses and their financial institutions. A criminal Indictment returned by a federal grand jury in Pittsburgh, USA charges ten members of the GozNym criminal network with conspiracy to commit the following: (i) infecting victims' computers with GozNym malware designed to capture victims' online banking login credentials; (ii) using the captured login credentials to fraudulently gain unauthorised access to victims' online bank accounts; (iii) stealing money from victims' bank accounts and laundering those funds using U.S. and foreign beneficiary bank accounts controlled by the defendants. Over the course of the international operation, searches were conducted in Bulgaria, Georgia, Moldova and Ukraine. Criminal prosecutions have been initiated in Georgia, Moldova, Ukraine and the United States." READ MORE

Source: Europol

Date: 3 May 2019

Double blow to dark web marketplaces

"Two prolific dark web marketplaces have been taken down in simultaneous global operations, supported by Europol: the Wall Street Market and the Silkkitie (known as the Valhalla Marketplace). Those responsible for the world's second largest illegal online market in the dark web, Wall Street Market, were also arrested in Germany, and two of the highest-selling suppliers of narcotics were arrested in US. Finnish authorities shut down Silkkitie earlier this year. When the same traders moved their activities to another illegal trade site on Tor, German authorities brought their illegal activities to an end" READ MORE

RELATED ARTICLES

Europol, DeepDotWeb shut down: administrators suspected of receiving millions of kickbacks from illegal dark web proceeds, 8 May 2019

Europol, Cryptocurrency laundering as a service: members of a criminal organisation arrested in Spain, 8 May 2019

Tech Republic, The Dark Web is smaller, and may be less dangerous, than we think, 6 May 2019

Source: US Department of Justice

Date: 9 May 2019

Nine individuals connected to a hacking group charged with online identity theft

"Six individuals connected to a hacking group known to its members as "The Community" were charged in a fifteen-count indictment unsealed today with conspiracy to commit wire fraud, wire fraud and aggravated identity theft, announced United States Attorney Matthew Schneider. In addition, a criminal complaint was unsealed charging three former employees of mobile phone providers with wire fraud in relation to the conspiracy. […] According to the indictment, the defendants are members of "The Community" and are alleged to have participated in thefts of victims' identities in order to steal cryptocurrency via a method known as "SIM Hijacking"." READ MORE

Source: BT

Date: 5 May 2019

No-deal Brexit 'could threaten evidence-sharing with Europe' on cyber crime

"Speedy European evidence-sharing about cybercrime may be endangered by a no-deal Brexit, a police officer in Northern Ireland has warned. European Investigation Orders (EIOs) allow the Police Service of Northern Ireland (PSNI) to access material within 90 days. The number of internet-related crimes has increased significantly in recent years, but the amount of resources devoted to tackling it is being outstripped, Detective Sergeant Darren McCracken said. He added: "If we leave as a result of Brexit we no longer have access to EIOs to obtain information within 90 days."" READ MORE

Source: The Guardian

Date: 5 May 2019

Inside Facebook's war room: the battle to protect EU elections

"Today the company admits it is under siege from billions of fake accounts trying to game its systems to win elections, make money or influence people in other ways, and battling a tsunami of fake news, disinformation and hate speech. Defeating them has become a matter of corporate survival, and Facebook wants users and regulators to know that it has stepped up those efforts. It also wants them to believe it is turning the tide. This week it took more than a dozen journalists to the Dublin "war room" at the heart of its efforts to protect European elections, to show off the resources it is pouring into protecting the continent-wide vote. Until the 23 May poll, and for several days after, about 40 people will be hunched over screens around the clock, monitoring the shifting pace of online conversation, looking for signs of manipulation, fake news or hate speech. They are backed up by a global network including threat intelligence experts, data scientists, researchers and engineers." READ MORE

Source: The National

Date: 15 May 2019

Papua New Guinea, Commerce and Industry Minister wants Parliament to ban Facebook for twelve months

"Commerce and Industry Minister Wera Mori says he will support any motion in Parliament to ban Facebook. He said too many Papua New Guineans were abusing it, "creating lies and malice". "I condemn the use of Facebook in this country," he said. He suggested that a 12-month ban should be imposed on users "so that people get their acts right and learn to use it better". "There needs to be some legislations governing it," he said." READ MORE

Source: El Economista

Date: 6 May 2019

Mexico, Diputados aumentan penas contraciberdelitos; envían reforma al Senado

"Con 403 votos a favor, ninguno en contra y ninguna abstención, la Cámara de Diputados aprobó el 30 de abril pasado, en lo general y en lo particular, la propuesta de decreto por la que se reforma el artículo 211 bis 1 del Código Penal federal que hace referencia al delito de hackeo, por el cual una persona, sin autorización, destruya, modifique o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad. Con esta reforma, que pasó para su votación a la Cámara de Senadores, las penas contra quien realice este delito se aumentarán desde seis meses a dos años de prisión y de 100 a 300 días de multa hasta de dos a cinco años y de 300 a 600 días de multa." READ MORE

Source: GhanaWeb

Date: 3 May 2019

Ghana lost US$105 million in 2018 through cybercrime

"Ghana lost US$105 million in 2018 through cybercrime such as mobile money fraud, various forms of intrusion and sextortion, Dr Gustav Yankson, Director of the Cybercrime Unit of the Criminal Investigation Department, Ghana Police Service, announced on Thursday. He added that the nation lost US$69 million in 2017 and US$35 million in 2016 respectively and thus, attributed the prevalence rate of cybercrime to individuals' attitudes and actions, which exposed their personal information to the public. "The cybercrime cases we received last year, fraud was number one constituting 60 per cent and followed by various forms of intrusion while sextortion placed third. "The indicators are that many people are so vulnerable to social engineering, meaning everything we're told, we believed it without cross-checking the source, and the mode of fraud is to deceive you using false pretences." READ MORE

Source: Bloomberg

Date: 2 May 2019

China's Mass Surveillance More Sophisticated Than Thought

"A mobile app used by police to track citizens in China's far west region of Xinjiang shows how some of the country's biggest technology companies are linked to a mass surveillance system that is more sophisticated than previously known, according to a report from Human Rights Watch. The app uses facial recognition technology from a firm backed by Alibaba Group Holding to match faces with photo identification and cross-check pictures on different documents, the New York-based group said on Thursday. The app also takes a host of other data points -- from electricity and smartphone use to personal relationships to political and religious affiliations -- to flag suspicious behavior, the report said." READ MORE

RELATED ARTICLES
BBC, Wikipedia blocked in China in all languages, 14 May 2019

Source: ZD Net

Date: 1 May 2019

Singapore urged to make changes to proposed bill against online falsehoods

"The Singapore government should make key amendments to its proposed law against online falsehoods to better reassure the public that it will not use the bill to stifle free speech and more clearly state the true intent of the act. As it stands, the draft Protection from Online Falsehoods and Manipulation Bill grants the government "far-reaching powers" over online communication which has created "significant concern". Such tools could be used by future governments "to suppress or chill debate and expression for political purposes", according to a statement jointly released on Tuesday by three Nominated Members of Parliaments (NMPs): Anthea Ong, Irene Quay, and Walter Theseira. NMPs are unelected MPs that were first introduced in 1990 as an avenue to allow citizens with no political party affiliation to participate in Singapore's parliamentary debates. First tabled in parliament last month, the proposed bill would require online sites to remove false information or show corrections to false and misleading claims. It also would allow government to order media platforms to shutdown fake accounts or bots that spread misinformation." READ MORE

Source: ASPI The Strategist

Date: 15 May 2019

Indonesia's democracy at risk from disinformation

"In the long lead-up to the world's largest ever single-day elections, disinformation ran rampant in Indonesia. It became so widespread that the government started holding weekly briefings to reveal 'hoaxes' and give the 'real facts'. Of particular concern was the rise in disinformation targeting Indonesia's electoral commission, the KPU. With the official results to be released by 22 May, how people react to this wave of disinformation could affect the short- and long-term stability of Indonesia's young democracy. […] Leading up to the 2019 election, both presidential campaigns funded teams of people to produce and disseminate disinformation using fake identities created for social media accounts. […] For some Indonesians, creating and sharing fake news became 'just a job', unrelated to ideological position or political motivation." READ MORE

Source: Daily Sabah

Date: 6 May 2019

Turkey's YSK rules for rerun of Istanbul mayoral elections

"Turkey's Supreme Election Council (YSK) has ruled for a rerun of local elections in Istanbul, the ruling Justice and Development Party (AK Party)'s YSK representative Recep Özel said Monday. […] A probe of irregularities found that dozens of members of balloting committees linked the Gülenist Terror Group (FETÖ), the group behind the 2016 defeated coup in Turkey. Of 43 committee members allegedly linked to FETÖ, 41 were found to be customers of Bank Asya, a FETÖ-linked bank, two were users of ByLock, the terror group's encrypted messaging app, and two were members of FETÖ-linked labor unions." READ MORE

Source: The Guardian

Date: 14 May 2019

WhatsApp urges users to update app after discovering spyware vulnerability

"WhatsApp is encouraging users to update to the latest version of the app after discovering a vulnerability that allowed spyware to be injected into a user's phone through the app's phone call function. The spyware was developed by the Israeli cyber intelligence company NSO Group, according to the Financial Times, which first reported the vulnerability. Attackers could transmit the malicious code to a target's device by calling the user and infecting the call whether or not the recipient answered the call. Logs of the incoming calls were often erased, according to the report." READ MORE

Source: ZD Net

Date: 14 May 2019

In a first, Israel responds to Hamas hackers with an air strike

"For the first time, Israel has used brute military force to respond to a Hamas cyberattack, three years after NATO proclaimed "cyber" an official battlefield in modern warfare. The "bomb-back" response took place on Saturday when Israel Defense Forces (IDF) launched an air strike against a building in the Gaza Strip. They claimed it housed Hamas cyber operatives, which had been engaging in a cyberattack against Israel's "cyberspace." […] Israeli officials did not disclose any details about the Hamas cyberattack; however, they said they first stopped the attack online, and only then responded with an air strike." READ MORE

Latest reports

- European Commission, Justice and Fundamental Rights, May 2019
- A. Diouf, Etude critique de la Stratégie Nationale de Cybersécurité en Sénégal, Apr 2019
- ETH Zurich – CSS Analyses in Security Policy, Public Attribution of Cyber Incidents, May 2019
- SWIFT, From security baseline to best practice – Securing India's critical channel infrastructure, 13 May 2019
- Ranking Digital Rights, 2019 RDR Corporate Accountability Index, May 2019

Upcoming events

- 14 -17 May, Ankara, Turkey – Introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors, iPROCEEDS
- 15-17 May, Bucharest, Romania – Meeting on Free Forensic Tools for the Law Enforcement Community (FREETOOL) in cooperation with UCD, iPROCEEDS, GLACY+, CyberSouth
- 16-17 May, San José, Costa Rica – Advisory mission on Procedural Legislation on Cybercrime and Electronic Evidence, GLACY+
- 16-17 May, Strasbourg, France – International Launching Conference of EndOCSEA@Europe Project, EndOCSEA@Europe
- 20-22 May, Manila, Philippines – Advisory mission and workshop on cybercrime and cyber security policies and strategies, GLACY+
- 22-24 May, Seoul, Korea – Participation in the 20th International Symposium on Cybercrime Response (ISCR 2019), GLACY+
- 20-25 May, Lisbon, Portugal – E-first course, European Cybercrime Training Education Group (ECTEG), CyberSouth
- 22-24 May, Windhoek, Namibia – Participation in the advisory mission on cybercrime legislation in the framework of the Cyber Resilience Program of the Commonwealth Secretariat, GLACY+
- 23-24 May, Manila, Philippines – Advisory mission on cybercrime reporting and workshop on collection and monitoring of criminal justice statistics on cybercrime and electronic evidence, GLACY+
- 27-31 May, Port Vila, Vanuatu – PILON Regional Workshop on cybercrime and electronic evidence in the Pacific. International Cooperation, GLACY+
- 28-29 May, Port Louis, Mauritius – Advisory mission on cybercrime reporting and workshop on collection and monitoring of criminal justice statistics on cybercrime and electronic evidence, GLACY+
- 28-30 May, Santo Domingo, Dominican Republic – Development of Cybercrime investigations, digital forensics capabilities and operating procedures on digital evidence for law enforcement agencies, combined with in-country workshops and advice on interagency cooperation and private public partnerships to fight cybercrime, GLACY+

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime