Cybercrime Digest

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

1-15 October 2020

Source: TechCrunch

Date: 6 Oct 2020

Europe's top court confirms no mass surveillance without limits

"In a ruling today the CJEU has made it clear that national security concerns do not exclude EU Member States from the need to comply with general principles of EU law such as proportionality and respect for fundamental rights to privacy, data protection and freedom of expression. However the court has also allowed for derogations, saying that a pressing national security threat can justify limited and temporary bulk data collection and retention — capped to 'what is strictly necessary'. While threats to public security or the need to combat serious crime may also allow for targeted retention of data provided it's accompanied by 'effective safeguards' and reviewed by a court or independent authority." READ MORE

RELATED ARTICLES

Court of Justice of the European Union, Press release, 6 Oct 2020

Source: Europol

Date: 15 Oct 2020

20 arrests in QQAAZZ multi-million money laundering case

"An unprecedented international law enforcement operation involving 16 countries has resulted in the arrest of 20 individuals suspected of belonging to the QQAAZZ criminal network which attempted to launder tens of millions of euros on behalf of the world's foremost cybercriminals. Some 40 house searches were carried out in Latvia, Bulgaria, the United Kingdom, Spain and Italy, with criminal proceedings initiated against those arrested by the United States, Portugal, the United Kingdom and Spain. The largest number of searches in the case were carried out in Latvia in operations led by the Latvian State Police (Latvijas Valsts Policija). Bitcoin mining equipment was also seized in Bulgaria. […] Comprised of several layers of members mainly from Latvia, Georgia, Bulgaria, Romania, and Belgium, the QQAAZZ network opened and maintained hundreds of corporate and personal bank accounts at financial institutions throughout the world to receive money from cybercriminals who stole it from accounts of victims. The funds were then transferred to other QQAAZZ-controlled bank accounts and sometimes converted to cryptocurrency using 'tumbling' services designed to hide the original source of the funds. After taking a fee of up to 50-percent, QQAAZZ returned the balance of the stolen funds to their cybercriminal clientele." READ MORE

Source: Europol

Date: 5 Oct 2020

COVID-19 sparks upward trend in cybercrime

"Europol's 2020 cybercrime report updates on the latest trends and the current impact of cybercrime within the EU and beyond. […] During the lockdown, we turned to the internet for a sense of normality: shopping, working and learning online at a scale never seen before. It is in this new normal that Europol publishes its 7th annual IOCTA. The IOCTA seeks to map the cybercrime threat landscape and understand how law enforcement responds to it. Although the COVID-19 crisis showed us how criminals actively take advantage of society at its most vulnerable, this opportunistic behaviour of criminals should not overshadow the overall threat landscape. In many cases, COVID-19 has enhanced existing problems." READ MORE

Source: IT Pro

Date: 1 Oct 2020

Less than 1% of computer hacking offences resulted in prosecution in 2019

"Of 17,600 reported cases of hacking in the UK only 57 led to prosecution in 2019, according to a new report. The numbers signify a 12% drop in convictions compared to 65 successful prosecutions the year before, according to legal firm RPC, which said police forces lack the resources to fully investigate all aspects of cyber crime. Government resources are instead being focused on large scale cyber attacks that are deemed a threat to national security, the firm suggested. As such, small, more niche hacking cases have proved elusive for the UK's police and judicial system. "Tracking down cybercriminals is a very resource-intensive task," said Richard Breavington, partner at RPC. "Hackers know how to cover their tracks, and doing so is relatively straightforward. Cyber criminals view hacking as a low-risk activity, with virtually zero risk of prosecution." RPC said that the majority of hacking offences reported in the UK are most likely carried out overseas, making it difficult to identify and pursue attackers who can route attacks through other jurisdictions where co-operation between law enforcement agencies is not always guaranteed." READ MORE

Source: Threat Post

Date: 13 Oct 2020

TrickBot Takedown Disrupts Major Crimeware Apparatus

"Microsoft and partners went after the botnet using a copyright infringement tactic and hunting down C2 servers. The TrickBot trojan has been dealt a serious blow thanks to a coordinated action led by Microsoft that disrupted the botnet that spreads it. However, researchers warn that the operators will quickly try to revive their operations. […] TrickBot is a well-known and sophisticated trojan first developed in 2016 as a banking malware – it has a history of transforming itself and adding new features to evade detection. Moving far beyond its banking roots, it has developed over the years into a full-fledged, module-based crimeware solution typically aimed at attacking corporations and public infrastructure. Users infected with the TrickBot Trojan will see their device become part of a botnet that can allow attackers to gain complete control of the device. Typical consequences of TrickBot infections are bank account takeover, high-value wire fraud and ransomware attacks. It's often seen working in concert with Emotet, another concerning and widespread trojan that's known for its modular design." READ MORE

Source: Council of Europe

Date: 5 Oct 2020

Cyber East: Technical Exercise for Georgian elections security completed

"The CyberEast project has completed the technical exercise for the stakeholders in Georgia, focusing on elections security. The exercise took place online between 5 to 7 October 2020 and involved representatives of the National Security Council, national CERT, State Security Service, National Communications Commission, Ministry of Defence, Cybercrime Unit of the Ministry of the Interior, as well as other stakeholders. The technical exercise was built on a realistic scenario, in which suspects prepared and launched DDOS and malware attacks on political parties and Central Electoral Commission of Georgia. The response to this attack comprised three stages of development, throughout which the participants were tasked to conduct Open Source Intelligence on Darknet, investigate cryptocurrency transactions, identify suspects through international cooperation mechanisms, and conduct DDOS and malware analysis through tools provided." READ MORE

Source: Council of Europe

Date: 9 Oct 2020

INTERPOL Malware Analysis Training, enhancing technical capacities of GLACY+ countries

"This training course is designed for cybercrime investigators from law enforcement agencies to establish technical knowledge and skills on static and dynamic analysis of malware for the purpose of understanding the behavior of malware in cybercrime scenarios, and further collect information or clues useful for attribution. […]The first of its series has been hosted between 5 – 9 of October 2020 for APAC region. GLACY+ countries are invited to the future events for Europe and Africa (23-27 November) and for Americas (7-11 December) later in 2020." READ MORE

Source: Council of Europe

Date: 6 Oct 2020

i-PROCEEDS-2: Online workshop and hands-on simulation for 24/7 points of contact in Serbia

"Under the framework of the Joint Project of the European Union and the Council of Europe – iPROCEEDS-2 a domestic workshop and hands-on simulation for improvement of the set-up, competencies and procedures of 24/7 points of contact in Serbia was organised online, on 06 October 2020. The workshop aimed at raising awareness on 24/7 points of contact in Serbia and to assess the use of the templates for requesting data as well as to identify new tools for improving the communication among the members of the Network. The workshop objectives were achieved through hands-on exercises, presentations and in-depth discussions." READ MORE

Source: Council of Europe

Date: 9 Oct 2020

Online training for the judicial sector in Turkey on countering online child sexual exploitation

"With the aim of providing the magistrates with further knowledge on the international legislation and the investigative powers that are used in investigations of OCSEA as well as with the particularities of this type of criminal activity, the training course was delivered in the framework of the iPROCEEDS-2 project and gathered over 100 magistrates. The programme of the training course covered fundamental issues on OCSEA: legislation, protection of the child victim or witness throughout criminal proceedings, particularities of gathering/handling electronic evidence when targeting online child sexual exploitation and particularities in this regard in the Turkish legislation and practices, and international cooperation mechanisms." READ MORE

Source: Council of Europe

Date: 14 Oct 2020

CyberSouth: National Workshop on cybercrime procedural law in Algeria

"The aim of this national workshop was to bring together the Algerian stakeholders responsible for drafting and enforcing cybercrime procedural law and assess whether the existing legislation follows the international human rights approach and rule of law standards. Representatives from the Ministry of Justice – magistrates and prosecutors dealing with cybercrime took part and contributed to the discussions. The activity helped the Algerian stakeholders to widen their understanding on the international standards on cybercrime procedural law and safeguards and to introduce their legislative tools and procedures for conducting cybercrime investigations and collection of e-evidence. Lastly, the participants received recommendations for the harmonisation of the national legislation with the international standards." READ MORE

Source: Council of Europe

Date: 2 Oct 2020

GLACY + & INTERPOL: Virtual Workshop On Data Protection And Global Policing Capabilities

"From 30 September to 2 October 2020, the GLACY+ Project held the Online Workshop on Data Protection and Global Policing Capabilities for 39 representatives from the police, judiciary and data protection community in Cabo Verde. The three-day workshop organized as part of the GLACY + (Global Action on Cybercrime Extended) project in collaboration with INTERPOL was delivered by instructors from the INTERPOL Data Protection Office in Lyon and Regional Bureau in Buenos Aires. Data protection is essential in international police cooperation and global sharing of police data. The workshop aimed to strengthen the understanding of the criminal justice community on how global trust can be built through robust data protection principles, and how INTERPOL effectively implements the principles and best practices in its daily activities of international policing." READ MORE

Source: INTERPOL

Date: 16 Oct 2020

Rising to meet the INTERPOL Digital Security Challenge

"A BEC scam was the premise of the fourth INTERPOL Digital Security Challenge – where teams of experts pool their knowledge and expertise in a race against the clock to investigate a simulated real-world cybercrime incident and gather evidence to identify the perpetrators. For the first time, the event was held virtually due to the COVID-19 pandemic. During the challenge, the 100 participating cybercrime and digital forensics experts from 50 countries had to analyse infected computers and contents of the BEC email messages received by the fictional company to uncover evidence of the malware used and the email servers which had been compromised. After linking the malware to a Command and Control (C2) server, the teams identified clues that would help narrow down the whereabouts of the cybercriminals and takedown the server. Adding an additional layer to the scenario, the criminals filmed the police takedown using drones and compromised the personal details of the officers involved. But one of the drones was captured, so the teams conducted digital forensic examinations to gather data from the device which identified the criminals' location. A computer seized at this location was also analysed for further information on the cybercriminals' activities." READ MORE

Source: Digital Times

Date: 6 Oct 2020

Ghana: National Cybersecurity Awareness Month Launched

"Ghana's Ministry of Communication in partnership with the National Cybersecurity Centre, an agency with the mandate to coordinate Ghana's cybersecurity development, has launched the fourth edition of the National Cybersecurity Month (NCSAM) in Accra. The month-long event is aimed at raising awareness on cybercrime in Ghana and online safety in Ghana, under the theme, "Cybersecurity on the Era of COVID 19." The Council of Europe is partnering with the event and the GLACY+ Project is supporting the organization of three activities in this context: two introductory trainings on cybercrime and electronic evidence for judges, prosecutors and law enforcement officers, and one workshop on the National Cyber Security Bill and its criminal justice aspects. READ MORE

Source: Ipandetec.org

Date: 8 Oct 2020

Nicaragua y su iniciativa de ciberdelitos

"La iniciativa de Ley Especial de Ciberdelitos sometida a aprobación de la Asamblea Nacional de Nicaragua el pasado mes de septiembre marca un antes y un después en materia de investigación, prevención y sanción de los delitos informáticos. A pesar de que Nicaragua no ha ratificado el Convenio de Budapest en el marco de la armonización de normas internacionales sobre el delito cibernético, su participación en foros y capacitaciones internacionales en materia de competencia cibernética y estrategias regionales en esta materia, urgían al Estado de Nicaragua la implementación de una legislación especial que regulará todo lo concerniente al delito informático y las pruebas electrónicas." READ MORE

Source: Fiji One News

Date: 4 Oct 2020

Fiji: "Having an open, secure, stable, accessible and peaceful cyberspace is vital for development."

"This message was conveyed at the opening of the Global Citizens Dialogue at the University of Fiji today by the Acting Permanent Secretary for Communications and Director-General Digital Government Transformation, Cybersecurity and Communications Ms Tupou'tuah Baravilala to the 125 participants. Today, 95% of all Fijians have access to internet connectivity and coupled with call charges, text and broadband rates being at the lowest prices that we have ever seen, at the highest speeds we've ever seen, it is clear that the internet has now become an integral part of our lives. […] Amongst Government's existing efforts to maintain a safe and secure cyber landscape, Ms Baravilala stated that the Cybercrime Bill which has been tabled in Parliament is aligned to the Budapest Convention – the only binding international instrument to address internet and computer crimes." READ MORE

Source: VoA

Date: 7 Oct 2020

Activists: Cambodia's Draft Cybercrime Law Imperils Free Expression, Privacy

"A recent draft of the cybercrime law obtained by VOA Khmer has drawn concerns from NGOs and rights groups over clauses that could help the government intensify its crackdown on freedom of expression, while also raising privacy and data collection concerns. The draft law, the formulation of which was first announced in 2010, was intended to regulate Cambodia's cyberspace, giving judicial police and courts access to investigate criminal infractions. However, an August draft of the law reveals that it could be used to further curtail freedom of expression while relying on vaguely defined scenarios to justify its implementation." READ MORE

Source: Manila Bulletin

Date: 7 Oct 2020

Philippines: DOJ tells public how to spot, avoid online banking scams

"The Department of Justice (DOJ) has issued an advisory on how the public could spot and avoid online banking scams. DOJ Office of Cybercrime (DOJ-OOC) Officer-in-Charge Charito Zamora issued the advisory on Tuesday, Oct. 6, "in light of the increasing reports from the general public involving phishing electronic mails (emails), vishing (voice/phone call), and smishing (SMS/text) in relation to online banking." "If you receive suspicious emails, text messages, or calls, immediately mark the emails as 'spam' and block the number that sent the message or made the call. Moreover, avoid opening or clicking any links, and downloading any attachments from suspicious and unverified senders." READ MORE

Source: Security Affairs

Date: 1 Oct 2020

North Korea-linked APT group targeted UN Security Council officials over the past year

A North-Korea-linked cyber espionage group has launched spear-phishing attacks aimed at compromising tens of officials from the United Nations Security Council. The campaign targeted at least 28 UN officials, including at least 11 individuals representing six countries of the UN Security Council. "According to information from another Member State, at least 28 individuals, including at least 11 officials from six members of the Security Council, became the targets of a spear-phishing campaign in 2020 which appeared to have been conducted by a Kimsuky advanced persistent threat group." reads the report." READ MORE

Source: Reuters

Date: 7 Oct 2020

Ukraine plan to tackle hackers sparks privacy fears

From crashing supermarket tills to messing with radiation readouts, Ukraine is hoping to tackle an ever-growing list of cyber-attacks with a new law that rights experts warn could give authorities excessive powers to pry into the lives of citizens. Last month, a group of lawmakers led by members of the ruling party proposed a set of laws that would, among other things, boost police search powers and require internet firms to store and provide access to large amounts of user data. READ MORE

Source: Security Affairs

Date: 12 Oct 2020

Researchers found alleged sensitive documents of NATO and Turkey

Researchers from the US-based firm Cyble recently came across a post shared by an unknown threat actor that goes online with the moniker Spectre123, where he has allegedly leaked the sensitive documents of NATO and Havelsan (Turkish Military/defence manufacturer). Cyble analysed the leaked sensitive documents and reported that they include Statement of Work files, proposals, contracts, 3d designs, resumes, excel sheets containing raw materials information, and financial statements. READ MORE

Latest reports

- Council of Europe, Digital solutions to fight COVID-19: shortcomings protecting privacy and personal data, 12 Oct 2020
- Council of Europe, Guidelines on electronic evidence in civil and administrative proceedings, 12 Oct 2020
- Europol, INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020, 5 Oct 2020
- Department of Justice and Equality of Ireland, Cybercrime: Current Threats and Responses - A review of the research literature, October 2020
- Africtivistes, Analyse des lois sur la cybercriminalité et sur la protection des données en Mauritanie, 1 Oct 2020
- Freedom House, Global Internet Freedom Declines in Shadow of Pandemic, 14 Oct 2020
- Welivesecurity by ESET, LATAM financial cybercrime: Competitors-in-crime sharing TTPs, 1 October 2020

Upcoming events

- 15-16 October, C-PROC/Moldova, (on-line), Assessment of crime proceeds/reporting systems, CyberEast
- 17-22 October, Germany, (on-line), Participation in ICANN 69 Conference, GLACY+
- 19 October, C-PROC/Tunisia (on-line), In-country workshop for developing guidelines on conditions and safeguards in cybercrime and e-evidence related investigation, CyberSouth
- 19-20 October, C-PROC/Ukraine, (on-line), Assessment of crime proceeds/reporting systems, CyberEast
- 19-20 October, C-PROC/Serbia, (on-line), Domestic workshops on cybersecurity, iPROCEEDS-2
- 19-23 October, C-PROC/ Ghana, (hybrid event), Training on Cybercrime & Electronic Evidence - 5 Day Training Session for Criminal Justice Sector (Northern Sector - Kumasi), GLACY+
- 19-30 October, C-PROC, (on-line), The International Symposium on Cybercrime Response (ISCR), GLACY+ 20 October, C-PROC, (on-line), Follow-up Webinar INTERPOL Digital Security Challenge Program (12-16 October) Online workshop, GLACY+
- 20 October, C-PROC/Jordan (on-line), In-country workshop for developing guidelines on conditions and safeguards in cybercrime and e-evidence related investigation, CyberSouth
- 20 – 21 October, UNDP Kosovo*(on-line): Virtual International Conference - Cybersecurity Threats Landscape, new trends and modes of cooperation, iPROCEEDS-2
- 26-30 October, C-PROC/Ghana, (hybrid event), Training on Cybercrime & Electronic Evidence - 5 Day Training Session for Criminal Justice Sector (Northern Sector - Accra), GLACY+27 October, C-PROC/Morocco, (on-line), In-country workshop for developing guidelines on conditions and safeguards in cybercrime and e-evidence related investigation, CyberSouth
- 27 October, C-PROC, (on-line), Webinar on the International Legal Framework on Cybercrime and Electronic Evidence (Internet Society Special Interest Group on Cyber Security), GLACY+
- 27 October, C-PROC/Ghana, (hybrid event), Workshop on draft Cybersecurity Bill with the NCSTWG/GLACY+ National Team/Criminal Justice Sector , GLACY+
- 27-28 October, C-PROC/ Chile, (on-line), Advisory workshop on judicial training strategies on cybercrime and electronic evidence, GLACY+

- 28 October, C-PROC/Lebanon, (on-line), In-country workshop for developing guidelines on conditions and safeguards in cybercrime and e-evidence related investigation, CyberSouth
- 28-29 October, C-PROC/ Montenegro: Domestic workshops on cybersecurity, iPROCEEDS-2
- By 31 October, C-PROC/ Albania, Desk review, Assessment of investigation and collection/ handling of electronic evidence under the respective domestic legislation, iPROCEEDS-2
- By 31 October, C-PROC/ Bosnia and Herzegovina, Desk review, Assessment of investigation and collection/ handling of electronic evidence under the respective domestic legislation, iPROCEEDS-2
- By 31 October, C-PROC/ Montenegro, Desk review, Assessment of investigation and collection/ handling of electronic evidence under the respective domestic legislation, iPROCEEDS-2
- By 31 October, C-PROC, Development of a guide on freezing and confiscation of virtual currencies and related assets, online, iPROCEEDS-2
- 30 October, C-PROC, (on-line), EU CyberNet annual conference, GLACY+
- By 31 October, C-PROC, Translation of Specialized Courses on International Cooperation and Electronic Evidence in FR, PT and ES, GLACY+
- By 31 October, C-PROC Translation of Introductory Judicial Training Materials in FR, PT and ES, GLACY+

Due to the COVID-19 pandemic outbreak and the countermeasures applied by most of the countries worldwide, in-country activities of the C-PROC capacity building initiatives foreseen in the month of August have been rescheduled to a later date.

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