Cybercrime Digest

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

01 – 15 August 2021

Cybercrime is Dangerous, but a New UN Treaty Could Be Worse for Rights

"[…] A global comprehensive treaty to counter cybercrime first proposed by Russia has gained enough support at the United Nations for negotiations to begin early next year. In addition to the irony of a government that faces criticism for turning a blind eye to cybercriminals operating within its borders pushing a global cybercrime treaty, the proposal is dangerous. […] Until now, there has been very little scrutiny of this process from a human right – as opposed to a geopolitical – perspective. A closer look at who is proposing the treaty, the way many states have defined "crime" in the cyber context, how efforts to fight cybercrime have undermined rights, and the shortcomings of multilateral negotiating processes reveals the dangers that this treaty process poses." READ MORE

RELATED ARTICLE:

Council of the European Union, EU priorities at the 76th United Nations General Assembly, 12 July 2021

Putin Is Crushing Biden's Room to Negotiate on Ransomware

"At the end of June, just before the White House scrambled to respond to another ransomware attack from Russia, Moscow presented a new international cyber treaty in the United Nations. Moscow has tightened its grip on the internet domestically for years and has recently pushed for a sovereign internet. […] The crux of the 69-page document is hardly shocking: The Putin regime is continuing its battle for a more closed, state-controlled internet. […] It purports to advance common ground between countries on cybersecurity, while the meaning of "cybersecurity" itself isn't even agreed upon. It promotes a broad range of requirements for technology companies under the guise of increasing stability in the cyber realm, when in reality it would encourage greater state censorship, surveillance, and control of the internet where countries are seeking more top cover to do so. […]" READ MORE

RELATED ARTICLE:

The Register, Russia tells UN it wants vast expansion of cybercrime offenses, plus network backdoors, online censorship, 3 August 2021

Unmasked: 23 charged over covid-19 business email compromise fraud

"On 10 August, 23 suspects were charged as a result of a series of raids carried out simultaneously in the Netherlands, Romania and Ireland. In total, 34 places were searched. These criminals are believed to have defrauded companies in at least 20 countries of approximately €1 million. The fraud was run by an organised crime group which prior to the COVID-19 pandemic already illegally offered other fictitious products for sale online, such as wooden pellets. Last year the criminals changed their modus operandi and started offering protective materials after the outbreak of the COVID-19 pandemic." READ MORE

Source: Convergencia digital

Date: 13 August 2021

Câmara tem relatório favorável para Brasil aderir a tratado global contra o cibercrime

"O Brasil até aqui não tinha aderido porque, apesar das loas de quem atua na persecução criminal, há situações complicadas. A primeira delas é (ou era antes de 2019) a tradição diplomática brasileira de não aderir a acordos dos quais o país não participou da elaboração. Além disso, apesar da maior integração no combate à criminalidade online, o tratado abre margem para vigilância governamental; permite que provedores de internet sejam obrigados a cooperar em buscas e apreensões eletrônicas, autoriza monitoramento remoto em tempo real, mesmo em nome de governos estrangeiros. E o que é muito pouco mencionado, mas atiça parte do apoio, é sobre o enforcement dos direitos autorais." READ MORE

Source: INTERPOL

Date: 06 Aug 2021

Guatemala: Global collaborative investigation nets suspected child sexual abuser

"A suspected prolific child sexual abuser has been arrested by Guatemalan law enforcement in a police operation supported by INTERPOL. In an investigation that began in February 2017, specialized law enforcement officers from around the world worked together through INTERPOL's International Child Sexual Exploitation (ICSE) database to identify eight child victims – aged approximately between seven and 17 years old – of a 45-year-old offender operating on the dark web. […] National investigators from Australia, Brazil, France and Switzerland cooperated with INTERPOL over years to comb through the substantial amount of child sexual abuse materials produced by this single offender over a 10-year period and piece together his identity as well as those of his victims." READ MORE

Source: Techradar

Date: 12 Aug 2021

Accenture hit by massive ransomware attack

"Accenture, counted amongst the world's largest IT consultancy firms, has confirmed that its network has been breached by the LockBit ransomware. […] Accenture is the latest of the high-profile victims of ransomware operators who are now actively targeting billion-dollar corporations. In fact, the number of ransomware attacks in 2021 has already surpassed last years' total since businesses aren't averse to paying the threat actors to prevent data leaks. '' READ MORE

RELATED ARTICLE:

Threatpost, Accenture Confirms LockBit Ransomware Attack, 11 August 2021

Source: Ars Tehnica

Date: 02 Aug 2021

Zoom to pay $85M for lying about encryption and sending data to Facebook and Google

"Zoom has agreed to pay $85 million to settle claims that it lied about offering end-to-end encryption and gave user data to Facebook and Google without the consent of users. The settlement between Zoom and the filers of a class-action lawsuit also covers security problems that led to rampant "Zoombombings." […] In addition to payments, Zoom "agreed to over a dozen major changes to its practices, designed to improve meeting security, bolster privacy disclosures, and safeguard consumer data," the settlement said. With the pandemic boosting its videoconferencing business, Zoom more than quadrupled its annual revenue from $622.7 million to $2.7 billion in the 12 months ending January 31, 2021. '' READ MORE

Source: ZD Net

Date: 05 Aug 2021

Researchers turn the spotlight on the hidden workers of the cybercrime world

"A collaborative research project by Czech Technical University in Prague, plus cybersecurity companies GoSecure and SecureWorks, analyzed the activities of people on the fringes of cybercrime, those behind projects like building the websites that end up being used for phishing attacks, affiliate schemes to drive traffic towards compromised or fake websites or writing the code that ends up in malware. […] "They are trying to earn a living and maybe crime is paying better so they go there, they drift into crime and come and go," said Sebastian Garcia, assistant professor at Czech Technical University, who argues that more attention needs to be paid to the people who dance the line between cybercrime and legal activity." READ MORE

Source: BBC News

Date: 06 Aug 2021

Apple to scan iPhones for child sex abuse images

"Apple has announced details of a system to find child sexual abuse material (CSAM) on US customers' devices. Before an image is stored onto iCloud Photos, the technology will search for matches of already known CSAM. Apple said that if a match is found a human reviewer will then assess and report the user to law enforcement. However there are privacy concerns that the technology could be expanded to scan phones for prohibited content or even political speech." READ MORE

Source: Threat Post

Date: 10 Aug 2021

1M Stolen Credit Cards Hit Dark Web for Free

"A dump of hundreds of thousands of active accounts is aimed at promoting AllWorld.Cards, a recently launched cybercriminal site for selling payment credentials online. Threat actors have leaked 1 million stolen credit cards for free online as a way to promote a fairly new and increasingly popular cybercriminal site dedicated to…selling payment-card credentials. […] The cards were published on an underground card-selling market, AllWorld.Cards, and stolen between 2018 and 2019, according to info posted on the forum." READ MORE

Source: The Guardian

Date: 02 Aug 2021

Pegasus spyware found on journalists' phones, French intelligence confirms

"French intelligence investigators have confirmed that Pegasus spyware has been found on the phones of three journalists, including a senior member of staff at the country's international television station France 24. […] France's national agency for information systems security […] relayed its findings to the Paris public prosecutor's office, which is overseeing the investigation into possible hacking." READ MORE

Source: Gobierno de Uruguay

Date: 06 Aug 2021

Desafíos de la ciberseguridad en Uruguay

"Papaleo resaltó el posicionamiento de Uruguay en materia de ciberseguridad, tras el reporte presentado por el Banco Interamericano (BID) y la Organización de los Estados Americanos (OEA) en 2020, en el que nuestro país se encuentra liderando la región en cuatro de las cinco dimensiones que presenta el informe. Señaló que, más allá de los avances, es necesario mejorar muchos aspectos como el marco regulatorio y la importancia de que Uruguay adhiera al Convenio de Budapest, en vigor desde 2004. […] También compartió algunos de los números extraídos del informe "Ciberseguridad en Uruguay" realizado en 2020 con el objetivo de analizar la situación en el país, fundamentalmente el mercado laboral, la demanda de servicios, las tendencias y los principales desafíos que enfrenta el sector.'' READ MORE

Source: FinteChile

Date: 03 Aug 2021

Las leyes pendientes en materia digital en Chile

"Nicolás Yuraszeck, socio de Magliona Abogados, profundiza lo anterior y relata que este proyecto viene a adecuar la legislación nacional al Convenio de Budapest suscrito por Chile en materia de delitos informáticos. […] Por otro lado, existe una iniciativa que busca fortalecer los derechos de los consumidores digitales, mejorando en el ejercicio de la garantía legal y dando una mayor equiparación en los contratos de adhesión.[…] Uno de los proyectos que con más ansias se espera es el Sistema Nacional de Ciberseguridad, iniciativa presentada por el Presidente Sebastián Piñera en la anterior cuenta pública." READ MORE

Source: Ministerio publico Costa Rica

Date:04 Aug 2021

Personal adquiere conocimientos sobre cooperación internacional, recepción e incorporación de prueba electrónica en casos de ciberdelincuencia

"Expertos del Departamento de Justicia de Estados Unidos, del Consejo de Europa y del Ministerio Público de Costa Rica imparten, desde ayer, la videoconferencia "Cooperación Penal Internacional", dirigida a 21 personas funcionarias de la institución. El objetivo es que estas comprendan el marco actual normativo y las prácticas utilizadas para la cooperación internacional bajo el Convenio de Budapest, sobre Ciberdelincuencia." READ MORE

RELATED ARTICLE:

Council of Europe, GLACY+: Specialized course on international cooperation for prosecutors and judges delivered in Costa Rica, 6 August 2021

Source: La Nación

Date: 10 Aug 2021

Paraguay: Identidad digital: un derecho que debe ser garantizado

"La oficina contra delitos informáticos del Ministerio Público tiene 2.500 causas abiertas por delitos digitales en lo que va de este año. Abarca desde aquellas pequeñas denuncias que tienen que ver con transferencias pequeñas de dinero vía internet o hasta el hackeo o la violación de grandes proyectos digitales o sistemas de seguridad en este ámbito. […] Para la fiscala Irma Llano, especializada en la lucha contra los delitos en este ámbito, la cuestión va mucho más allá de las cuestiones cercanas e implica una nueva forma de comportamiento de las personas en cuanto a su seguridad en internet y sobre todo en las redes sociales." READ MORE

Source: Le Faso

Date: 10 Augl 2021

Cybercriminalité au Burkina: Un préjudice de 1 milliard 400 millions de francs CFA entre mai 2020 et juin 2021

"Une vingtaine de journalistes prennent part les 10 et 11 août 2021 à Ouagadougou à un séminaire de sensibilisation sur la cybercriminalité. Organisée par la Brigade centrale de lutte contre la cybercriminalité (BCLCC), structure placée sous la tutelle du ministère de la Sécurité, cette rencontre vise à impulser l'implication des médias nationaux dans la lutte contre la cybercriminalité en vue d'une réponse efficace." READ MORE

Source: Cio Mag

Date: 03 Aug 2021

« Et si on parlait numérique ? », une rencontre bimestrielle avec les acteurs du numérique

"Au Bénin, le Ministère du numérique et de la digitalisation a initié une rencontre périodique entre les acteurs de l'écosystème numérique et les journalistes spécialisés du secteur. […] Selon le classement 2020 du Global Cybersecurity Index, le Bénin est classé 6e sur 44 pays en Afrique. Cet indice de l'Union internationale des télécommunications (UIT) analyse l'engagement des Etats en matière de cybersécurité et la sensibilisation de leurs populations." READ MORE

Source: Council of Europe

Date: Aug 2021

CyberEast Interview: The application of the UCD Forensic Computing and Cybercrime Investigation master programme in the work of combating online child sexual exploitation and abuse of children

"In this interview you can meet Artur Degteariov working with the General Inspectorate of Moldovan Police fighting online child sexual exploitation and abuse of children. Artur is also a master student in the Master programme MSc Forensic Computing and Cybercrime Investigation offered by the University College Dublin, in Ireland, through the CyberEast project, and a long-term country team member of the CyberEast project driving progress on cybercrime in the Eastern Partnership region." READ MORE

Source: Bleeping computer

Date: 03 Aug 2021

Ransomware attack hits Italy's Lazio region, affects COVID-19 site

"The Lazio region in Italy has suffered a reported ransomware attack that has disabled the region's IT systems, including the COVID-19 vaccination registration portal. Early Sunday morning, the Lazio region suffered a ransomware attack that encrypted every file in its data center and disrupted its IT network. […] While ransomware gangs are known to steal data during an attack as leverage in extortion attempts, the region states that health, financial, and budget data are safe. […] Italian security researcher JAMESWT stated that there is evidence in Italy that the attack was conducted by LockBit 2.0 but could not share further information." READ MORE

Source: Bitkom

Date: 05 Aug 2021

Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr

"Durch Diebstahl, Spionage und Sabotage entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von 223 Milliarden Euro. […]Die Schadenssumme ist mehr als doppelt so hoch wie in den Jahren 2018/2019, als sie noch 103 Milliarden Euro p.a. betrug. Neun von zehn Unternehmen (88 Prozent) waren 2020/2021 von Angriffen betroffen.[…] Sie sind meist unmittelbare Folge von Ransomware-Angriffen. Durch sie werden Computer und andere Systeme blockiert, anschließend werden die Betreiber erpresst. Die so verursachten Schäden haben sich im Vergleich zu den Vorjahren 2018/2019 mehr als vervierfacht (+358 Prozent)." READ MORE

Latest reports

- INCIBE: TemáTICas: aspectos clave para teletrabajar de forma segura, 03 August 2021
- Market reports, Cybercrime and Security Market and its Future Outlook During Forecast Period of 2020-2026, 4 August 2021
- LUMEN, Charting The Real-World Application Of CTFs, 4 August 2021
- Virginia Tech Hume Center, Use and abuse of personal information, 4 August 2021
- Scoop Byte, How To Avoid Cybercrime in the iGaming Industry?, 5 August 2021
- Center for global develpment, Do Evolving Digital Trade Rules Create an Uneven Playing Field? Understanding Global Perspectives, 9 August 2021
- Cornwell , A cross-domain qualitative meta-analysis of digital forensics: Research trends, challenges, and emerging topics, 10 August 2021
- Schneier on Security: Apple Adds a Backdoor to iMessage and iCloud Storage, 10 August 2021
- CompariTech, Cybercrime victims lose an estimated $318 billion annually, 11 August 2021
- Schneier on Security: Using AI to Scale Spear Phishing, 13 August 2021
- AlSur, Un marco jurídico de derechos humanos para la vigilancia de las comunicaciones en América Latina, 2021
- AlSur, Violencia política de género en internet, 2021
- Carbon Black, Global Incident Response Threat Report: Manipulating Reality, August 2021

Upcoming events

- 16 – 19 August, Bucharest, Romania, Regional meeting on Council of Europe developed Guide on seizing cryptocurrencies and practical exercise on seizing virtual assets, iPROCEEDS-2
- 26 August, Kosovo*[1] (online), Domestic workshop on MLA practices on country level, alignment of procedures with the Budapest Convention and its Second Additional Protocol, iPROCEEDS-2
- 31 August – 2 September, Turkey (online), Domestic practical exercise for developing skills on cooperation on cybercrime and electronic evidence for judicial, police and cybersecurity authorities with service providers, iPROCEEDS-2
- August – September, Desk Analysis, Study on COVID-19 related cybercrime in Asia, Octopus Project.

Due to the COVID-19 pandemic outbreak and the countermeasures applied by most of the countries worldwide, some 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

---

[1] *This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.