Cybercrime Digest

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

15 – 31 December 2021

Source: G7

Date: 22 Dec 2021

G7 Interior and Security Ministers – Extraordinary Senior Officials' Forum on Ransomware

"On 15-16 December, in line with the commitment made at the Interior and Security Ministers' meeting in September 2021, G7 Senior Officials gathered virtually for an Extraordinary Senior Officials' forum on ransomware, along with representatives from the Council of Europe; European Commission; European Union Agency for Cybersecurity, Europol; Financial Action Task Force; G7 Cyber Expert Group; Global Forum on Cyber Expertise; Interpol and the United Nations Office on Drugs and Crime. [...] Earlier in the year, G7 leaders called on states to identify and disrupt ransomware criminal networks operating from within their borders at pace and hold those networks accountable for their actions." READ MORE

Source: CTV News

Date: 22 Dec 2021

Predators use SnapChat app for child luring, sexual exploitation

"New data reveals an alarming trend where teenagers are being sexually exploited on the popular app, SnapChat. Cybertip, an online tip reporting site for child sexual abuse and exploitation, has documented 27 of these types of incidents in the past six months. More recently, these engagements include predators hacking into accounts or using threats to share intimate images. "The fact that kids are on so many different apps and technology, social media sites, it's really easy to engage with them," said Stephen Sauer, Canadian Centre for Child Protection. The agency found the main targets are boys between the ages of 15 and 17." READ MORE

Source: The Stack

Date: 29 Dec 2021

Christmas pay for police, nurses at risk after Kronos hit by ransomware

"One of the world's biggest workforce management software companies, Kronos, has been hit by ransomware in an attack that has left multiple public and private sector customers reliant on its software reeling. The hack looks likely to leave thousands, including nurses, without critical paychecks ahead of Christmas. Multiple Kronos software platforms used by millions have been unavailable since December 11. […] Data centres in the US, Frankfurt, and Amsterdam were hit in the attack, the company said." READ MORE

RELATED ARTICLES:

Hea!thcare Innovation, Sector Within Public Finance Most Impacted by Kronos Ransomware is Healthcare, 23 December 2021

Becker's Heath IT, Baptist Health, Allegheny & 5 other hospitals, health systems affected by Kronos ransomware attack, 15 December 2021

The Stack, Kronos outage latest: Attackers took down connection to backups, January 2022

Source: bbc.com

Date: 20 Dec 2021

UK donates 225 million stolen passwords to hack-checking site

"UK law enforcement has donated a tranche of 225 million unique passwords to a cyber-security project helping to protect users from hacking. The National Crime Agency (NCA) recovered the database from cyber-criminals who had collected real users' email addresses and passwords. That list has been added to free online service Have I Been Pwned (HIBP). It lets anyone search through hundreds of millions of passwords to see if theirs is in the hands of criminals." READ MORE

Source: the Record

Date: 15 Dec 2021

French police detain suspect who laundered €19 million in ransomware payments

"French authorities have arrested a suspect this week for allegedly laundering more than €19 million (~$21.4 million) in ransomware payments. […] The arrest this week comes as law enforcement agencies across the world have begun collaborating and cracking down on ransomware operations after years of repeated attacks, some of which have crippled government agencies and private sector companies time and time again." READ MORE

Source: POLICE1.COM

Date: 28 Dec 2021

How law enforcement can use digital technology to intercept human trafficking

"According to the Trafficking in America Taskforce, forced labor generates a total of approximately $150 billion per year in illegal profits in the private economy. Of this figure, about $99 billion comes from commercial sexual exploitation. [...] One of the critical strategic resources available to both law enforcement agencies and NGOs is digital intelligence (DI) technology. [...] To stop trafficking on a larger scale, agencies need the tools and training to lawfully collect digital evidence and trace traffickers to their wider syndicates. Having digital intelligence solutions in the hands of law enforcement is critical to upscaling these efforts and reversing the tide. " READ MORE

Source: The Daily Swig

Date: 21 Dec 2021

Survey scams rekindled using advertising industry tricks to deliver tailor-made assaults

"Cybercriminals are using new targeted tools and techniques to revive an online scam that had, until recently, fallen out of fashion. The wide-ranging campaign, targeting users in 90 countries around the world, uses fake surveys and giveaways purporting to be from popular brands to steal users' personal and payment data." READ MORE

Source: Contrareplica

Date: 29 Dec 2021

Mexico: Diputada de Morena propone expedir leyes en materia de ciberseguridad y cibercrimen

"La diputada Juanita Guerra Mena (Morena) planteó una iniciativa de reforma constitucional que pretende facultar al Congreso de la Unión para expedir ordenamientos legales en materia de ciberseguridad y cibercrimen. En un comunicado, detalló que esta propuesta adiciona la fracción XXIII Ter al artículo 73 de la Carta Magna, a fin de crear normas que contengan mecanismos que establezcan una coordinación entre autoridades de los tres órganos de gobierno y se diseñe una estrategia nacional de inteligencia cibernética y policial." READ MORE

Source: Techstory.in

Date: 25 Dec 2021

UAE Introduces 5-Year Jail Time and Fines for Crypto Criminals

"UAE has introduced stringent new laws to shield the public from financial fraud. The new laws will put up a rather strong barrier for those criminals involved in cryptocurrency scams. If caught red-handed, they will have to face five years in jail. This is in addition to the fines that run up to Dh1 million. These new laws are a part of the legal reforms which were announced by President Sheikh Khalifa earlier last month." READ MORE

RELATED ARTICLE:

The SIASAT Daily, UAE's cybercrime law: Illegal to click pictures without consent, 28 Dec 2021

Source: SaudiGazette.com

Date: 30 Dec 2021

Saudi Arabia: Law of Evidence allows courts to use digital means to elicit evidence

"The Law of Evidence, approved recently by the Council of Ministers, consists of several provisions that bring about qualitative leap in the procedures with regard to various aspects of presenting, examining and taking decisions on the evidence at the courts and other judicial institutions in the Kingdom. […] The law stipulates clear-cut mechanism for interrogation and presenting testimony of deaf and dumb people. The law ensures that all the facts have to be vindicated with substantial evidence so as to enable the judge to issue a sound and fool proof verdict in the case." READ MORE

Source: NDTV.COM

Date: 31 Dec 2021

India: 'Free Omicron Test' Offered Online Is A Cybercrime, Says Home Ministry

"Amid a rise in Omicron cases, the Ministry of Home Affairs (MHA) has issued an advisory against cybercriminals targeting potential victims by offering them free tests for detecting Omicron variant of COVID-19. The cyber and information security division of MHA has issued an advisory that read: "Cybercriminals are taking advantage of lowering of cyber defences due to the shift of focus to the health crisis. Cybercriminals are always finding new ways to defraud citizens. As nowadays Omicron variant themed cybercrimes are increasing every day. Cybercriminals are employing various tactics to perpetrate cybercrimes to capitalize on the rapidly evolving situation to defraud innocent victims." READ MORE

RELATED ARTICLE:

LiveMint.com, 'Cybercriminals are taking advantage', Centre warns against fraud sites amid Omicron surge, 31 December 2022

Source: Inquirer.Net

Date: 29 Dec 2021

Philippines: DOJ received 2.8 million online child sex abuse complaints in 2021

"The Department of Justice (DOJ) has received more than 2.8 million reports about online child sexual abuse this year, more than double the nearly 1.3 million reports it collated in 2020. In its annual report, the DOJ's Office of Cybercrime (OOC) said it launched an official investigation of 268 cases of online sexual exploitation of children this year, almost four times the 73 cases it handled in 2020." READ MORE

Source: Council of Europe

Date: 17 Dec 2021

CyberEast: Fourth Steering Committee of the Project

“More than 60 project country team members, project partners and Cybercrime Programme Office staff took part in this virtual meeting, aiming to hear directly from project countries on the impact of the project, especially under the COVID-19, the review of the progress of CyberEast in 2021 since the third Steering Committee, as well as to discuss and approve the revised Workplan for 2022.” READ MORE

Source: osce.org

Date: 27 Dec 2021

OSCE trains law enforcement and criminal justice officials in Armenia on combatting and preventing cybercrime

“About twenty police officers, prosecutors, and representatives of the National Security Service and Investigative Committee of Armenia attended a training course on open-source IT forensics and network investigations held from 20 to 24 December 2021 at the Academy of Justice in Yerevan. The OSCE and the Council of Europe jointly organized the event, with the support of the Ministry of Foreign Affairs of Armenia.” READ MORE

Source: politico.eu

Date: 20 Dec 2021

Belgian defense ministry hit by cyberattack

“Belgium's ministry of defense confirmed on Monday it had been hit by a cyberattack. Hackers exploited a vulnerability in software called Log4j, which was discovered earlier in December, a ministry spokesperson told local media. The ministry uncovered the attack last Thursday. Cybersecurity officials across the world have rushed to patch the Log4j vulnerability over the past week. The glitch has affected a long list of software firms including Amazon and Microsoft.” READ MORE

Source: incyber.fr

Date: 29 Dec 2021

France: La police se dote d’une base de données sur les cybercriminels

“En France, la police et la gendarmerie vont disposer d’un nouvel outil pour faciliter l’identification des cybercriminels : baptisée Malware Information Sharing Platform – Police Judiciaire (MISP-PJ), il s’agit d’une base de données regroupant des informations sur les auteurs de cyberattaques. Un arrêté du 22 décembre 2021 acte la création de cette base. Les données de MISP-PJ sont issues essentiellement des logiciels de rédaction des procédures judiciaires de la police nationale (LRPPN) et de la gendarmerie nationale (LRPGN), ainsi que du recueil d’informations relatives aux incidents de sécurité sur les réseaux et systèmes d’information du Centre d’alerte et de réaction aux attaques informatiques de la police judiciaire (CSIRT-PJ).” READ MORE

Latest reports

- European Union Agency for Fundamental Rights, Unaccompanied children outside the child protection system, 2021
- UNESDOC, Tackling cyber bullying and other forms of online violence involving children and young people, 2021
- IFSH, New IFSH Policy Brief: Cybercrime: Working together to Mitigate Peace and Security Threats, 20 December 2021
- Eurojust, New version of practical guide on joint investigation teams for practitioners, 22 December 2021
- Springer link, Cyberbullying detection: advanced preprocessing techniques & deep learning architecture for Roman Urdu data, 22 December 2021
- Government Tech, The top 22 security predictions for 2022, 23 December 2021
- UK Home Office, Group-based child sexual exploitation characteristics of offending (accessible version), 23 December 2021
- Hacked, 2021: A Year in Cybercrime, 25 December 2021
- SAGE journals, Low self-control and cybercrime victimization: an examination of indirect effects through risky online behavior, 26 December 2021
- The National News, Top 10 cybercrime trends to watch for in 2022, 29 December 2021
- CNN Espanol, Desde los inicios del metaverso hasta ciberataques: 5 tendencias tecnológicas que impactarán en 2022, 29 December 2021
- Cybercrime Magazine, Top 6 cybersecurity predictions and statistics for 2021 to 2025, 30 December 2021
- AOCSafeEnvironment, Offenders can be anyone: why knowing the signs is important, 31 December 2021
- Varonis, 134 Cybersecurity Statistics and Trends for 2022, 2 January 2022

The Cybercrime Digest appears bi-weekly. The news is selected by relevance to the current areas of interest to C-PROC and does 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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE