Cybercrime Digest

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

1 – 15 January 2022

Source: BBC

Date: 15 Jan 2022

REvil ransomware gang arrested in Russia

"Authorities in Russia say they have dismantled the ransomware crime group REvil and charged several of its members. The United States had offered a reward of up to $10m (£7.3m) for information leading to the gang members, following ransomware attacks. Russia's intelligence bureau FSB said the group had "ceased to exist" […] The agency said it had acted after being provided with information about the REvil gang by the US. According to the Russian state news service Tass, REvil "developed malicious software" and "organised the theft of money from the bank accounts of foreign citizens". The FSB said it had seized more than 426 million rubles (£4m), including about £440,000 worth of crypto-currency." READ MORE

RELATED ARTICLES:

Krebs on Security, At Request of U.S., Russia Rounds Up 14 REvil Ransomware Affiliates, 14 January 2022

Source: EFF

Date: 13 Jan 2022

Nearly 130 public interest organisations and experts urge the United Nations to include human rights safeguards in proposed UN Cybercrime Treaty

"EFF and Human Rights Watch, along with nearly 130 organizations and academics working in 56 countries, regions, or globally, urged members of the Ad Hoc Committee responsible for drafting a potential United Nations Cybercrime Treaty to ensure human rights protections are embedded in the final product. […] In a letter to the committee chair, EFF and Human Rights Watch along with partners across the world asked that members include human rights considerations at every step in the drafting process. We also recommended that cross-border investigative powers include strong human rights safeguards, and that global civil society be provided opportunities to participate robustly in the development and drafting of any potential convention." READ MORE

RELATED ARTICLES

Human Rights Watch: Letter to the UN Ad Hoc Committee on Cybercrime | Human Rights Watch, 13 Jan 2022

Source: Euronews

Date:14 Jan 2022

COVID lockdowns saw a record rise in online child sexual abuse reports, says watchdog

"Last year was the worst year on record for child sexual abuse online, the Internet Watch Foundation (IWF) has said, as pandemic-related lockdowns saw younger and younger children being targeted "on an industrial scale" by internet groomers. The UK-based charity took action against 252,000 URLs in 2021 which it confirmed contained images or videos of children being raped and suffering sexual abuse. In total, IWF analysts investigated 361,000 reports of suspected criminal material last year, including tip offs from the public. This is more than they dealt with in the entire first 15 years of the charity's existence when they assessed 335,558 reports from 1996 to 2011. The IWF also reported a threefold increase in content showing the abuse of children aged between seven and 10 years old." READ MORE

Source: Infosecurity

Date: 14 Jan 2022

Ukrainian Cops Bust Suspected $1m Cybercrime Ring

"Ukrainian police have swooped on five suspected members of a ransomware affiliate that targeted dozens of foreign companies and made at least $1m in profits. Officers from the country's Cyber Police Department and the Security Service (SBU), teamed-up with law enforcers in the US and UK to track down the gang, which is said to have hit more than 50 companies in Europe and America. […] According to Ukrainian police, the group targeted companies with phishing emails laden with ransomware. They also sold IP address-spoofing services to other hackers to help them stay hidden while launching ransomware, information theft, DDoS and other attacks, the SBU said." READ MORE

Source: Euronews

Date: 11 Jan 2022

Europol told to delete personal data not linked to any crime by EU watchdog

"Europol has been ordered to delete any information related to individuals who have not been found guilty of any crime. An investigation found that the European Union's police agency had collected and stored data on innocent citizens. Europol was told to delete any data that did not comply with safeguards on the length of time that sensitive information can be stored, where data can only be stored for six months if no criminal activity can be proven. The European Data Protection Supervisor said that Europol was notified of the order on 3 January following a 2019 inquiry." READ MORE

Source: Europol

Date: 14 Jan 2022

Europol's Statement on the Decision of the European Data Protection Supervisor

"The EDPS Decision will impact Europol's ability to analyse complex and large datasets at the request of EU law enforcement. This concerns data owned by EU Member States and operational partners and provided to Europol in connection with investigations supported within its mandate. It includes terrorism, cybercrime, international drugs trafficking and child abuse, amongst others. Europol's work frequently entails a period longer than six months, as do the police investigations it supports. This is illustrated by some of Europol's most prominent cases in recent years." READ MORE

Source: Logistics Manager

Date: 12 Jan 2022

Threat of cybercrime looms large for supply chains, according to World Economic Forum

"Growing cyber threats have been listed among the greatest global risks in the annual World Economic Forum Global Risks Report, published yesterday. [...] The report cited specifically the "growing dependency on digital systems" – intensified by the response to Covid-19 – which has "fundamentally altered societies". At the same time, cybersecurity threats are growing and outpacing societies' ability to effectively prevent or respond to them. Attacks on critical infrastructure, misinformation, fraud and digital safety will impact public trust in digital systems and increase costs for all stakeholders. As attacks become more severe and broadly impactful, already-sharp tensions between governments impacted by cybercrime and governments complicit in their commission will rise as cybersecurity becomes another wedge for divergence, rather than cooperation, among nation states." READ MORE

Source: Infosecurity

Date: 11 Jan 2022

Corporate Cyber-Attacks Spike 50% in 2021

"Global weekly cyber-attacks hit an all-time high in Q4 2021 of 925 attempts per organization, according to new data from Check Point. The security vendor analyzed information collected by hundreds of millions of global sensors from its Threat Prevention products across networks, endpoints and mobiles. It claimed attempted attacks have been continuously increasing since Q2 2020, with 50% more attacks seen per week on corporate networks in 2021 compared to 2020. The education and research sector experienced the highest volume of attacks during 2021, amounting to an average of 1605 per organization every week, a 75% increase on 2020. It was followed by government/military with 1136 attacks, up 47% year-on-year, and communications with 1079, up 51%. Africa experienced the highest volume of weekly attacks in 2021, with an average of 1582 per organization, a 13% increase from 2020. However, European organizations experienced the most significant increase in weekly attacks, up 68% to 670, according to the report." READ MORE

Source: Cybernews

Date: 14 Jan 2022

Ukrainian government hit by cyberattack

"Friday morning, Ukrainian government websites were hit by a major cyberattack. "All your data has been uploaded to the web. All data on the computer is destroyed and cannot be recovered. All information about you has become public. Fear and prepare for the worst. This is for your past, present, and future," reads a message on the Ukrainian foreign ministry website. Malicious hackers posted a warning in Ukrainian, Russian, and Polish. The government websites are down and cannot be reached at the moment. It seems that most of the websites belonging to different ministries are down, with some exceptions." READ MORE

RELATED ARTICLE:

Reuters, Massive cyberattack hits Ukrainian government websites as West warns on Russia conflict, 14 January 2022

Source: BBC

Date: 14 Jan 2022

Largest darknet stolen credit card site closes

"The administrators of the largest illegal marketplace on the darknet for stolen credit cards are retiring after making an estimated $358m (£260m). The anonymous owners of UniCC thanked the criminal fraternity for their business, citing age and health for the closure. Many other illegal darknet marketplaces have also shut down voluntarily over the winter for unknown reasons. Police say the trend leaves them with mixed feelings." READ MORE

Source: Security Week

Date: 13 Jan 2022

Report: Dozens of El Salvador Journalists, Activists Hacked

"Dozens of journalists and human rights defenders in El Salvador had their cellphones repeatedly hacked with sophisticated spyware over the past year and a half, an internet watchdog said Wednesday. Reporting on its latest findings about use of the Israeli firm NSO Group's Pegasus spyware, the University of Toronto's Citizen Lab said it had identified a Pegasus operator working almost exclusively in El Salvador in early 2020." READ MORE

RELATED ARTICLE:

BBC, El Salvador journalists and activists hacked with spyware, report says, 13 January 2022

Source: Italy News24

Date: 4 Jan 2022

Nightmare cybercrime in Italy. The Postal Police: online fraud for 36 million, child pornography record

"It emerges from the financial statements published by the Postal and Communications Police according to which the turnover of financial cybercrime continues to grow. In fact, in 2021 they registered 126 cyber attacks on the financial systems of large and medium-sized enterprises, for a total amount of over 36 million of euro illegally stolen through complex telematic fraud; 17 of these millions have been recovered thanks to the intervention of the Postal Police. […] According to the investigators, "attacks on the corporate world through fraud based on social engineering techniques are particularly evident conditioned by the pandemic in progress, especially for the widespread use of communication systems for remote economic management, resulting from the large-scale adoption of smart-working"." READ MORE

Source: Economistjurist

Date: 1 Jan 2022

Ciberdelincuencia tras el coronavirus: tres claves para saberlo todo

"Todos tenemos más o menos claro que existe eso que llaman la Ciberdelincuencia y que cada día está más cerca de nosotros, ¿verdad? Todos hemos escuchado hablar de ella, ya sea por los medios de comunicación, por personas de nuestro entorno que han sufrido algún ciberdelito o, incluso, porque nosotros mismos hemos sufrido alguno de ellos." READ MORE

Latest reports

- Scientific American, Hacking the ransomware problem, 1 January 2022
- Institute for Security Studies, Africa must get up to speed on cyber diplomacy, 3 January 2022
- Africa Center, Deluge of Digital Repression Threatens African Security, 4 January 2022
- TechCrunch, Opportunity not fear: Reframing cybersecurity to build a safer net for all, 4 January 2022
- FORBES, Predicting What 2022 Holds For Cybersecurity, 6 January 2022
- World Economic Forum, Global Risks Report 2022, 11 January 2022
- AODB, Vers un cloud souverain français, 12 January 2022
- Cyberpsychology, Behavior, and Social Networking, Virtual Reality Program in Cybercrime Investigation: A Pilot Study Examining Search and Seizure of Digital Evidence Practice, 12 January 2022
- Cyberint, 2022 Cybersecurity Predictions - Cyberint, 12 January 2022
- Cybernews, Anti-phishing training may make people more likely to fall victim to phishing, 13 January 2022
- Cybernews, North Korean hackers stole $400 million in cryptocurrency in 2021, 14 January 2022

Upcoming events

- 17-20 January, C-PROC/AFRICA, (*online*), Attending the Commonwealth Secretariat Regional Workshop on addressing cybercrime in Sub-Saharan Africa, GLACY+
- 17-28 January, C-PROC/MULTIPLE COUNTRIES, *(hybrid),* Attending the Ad Hoc Committee on new UN Treaty, GLACY+, OCTOPUS, CyberEast, iPROCEEDS-2
- 18 January, C-PROC/MULTIPLE COUNTRIES, *(online),*Second series of monthly thematic webinars for the International Network of the National Judicial Trainers, GLACY+
- 18-27 January, C-PROC/CARICOM IMPACS, (*online*), A series of online cybercrime trainings for Caribbean magistrates and prosecutors, OCTOPUS
- 19-21 January, ARMENIA, (*in-person),* Training on interagency cooperation and financial investigations / intelligence (in cooperation with OSCE), CyberEast
- 20 January, C-PROC/ALBANIA, *(online),* Domestic workshop on cybersecurity, iPROCEEDS-2
- 21 January, C-PROC, (*online*), C-PROC training session on the online training platform for cybercrime and electronic evidence, OCTOPUS
- 24-25 January, C-PROC/TURKEY, *(online),* Workshop on Council of Europe's developed Guide for first responders to cybercrime investigations for Turkish law enforcement professionals, iPROCEEDS-2
- 25-January, C-PROC/MULTIPLE COUNTRIES, *(online),* 11th Project Steering Committee, GLACY+
- By 25 January, C-PROC, (*desk study),* Study on COVID-19 related cybercrime in the Philippines, OCTOPUS
- By 31 January, C-PROC, (*desk study),* Updating a series of country wikis for the Octopus platform, OCTOPUS
- By 31 January, C-PROC, (*desk study),* New materials for the Advanced Judicial Course on Cybercrime and Electronic Evidence, GLACY+
- January-February, C-PROC/GEORGIA, *(online*), Development of revised Georgian Information Security Law, CyberEast

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 January have been rescheduled to a later date.

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