Cybercrime Digest

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

16 – 31 July 2022

Source: Council of the European Union

Date: 19 July 2022

Declaration by the High Representative on behalf of the European Union on malicious cyber activities conducted by hackers and hacker groups in the context of Russia's aggression against Ukraine

"Russia's unprovoked and unjustified military aggression against Ukraine has been accompanied by a significant increase of malicious cyber activities, including by a striking and concerning number of hackers and hacker groups indiscriminately targeting essential entities globally. This increase in malicious cyber activities, in the context of the war against Ukraine, creates unacceptable risks of spillover effects, misinterpretation and possible escalation. In this regard, we recall the EU and its Member States' strong condemnation of the cyber-attacks against Ukraine on 14 January 2022, and the attribution on 10 May 2022 of the malicious cyber activity targeting the satellite KA-SAT network to the Russian Federation. The latest distributed denial-of-service attacks against several EU Member States and partners claimed by pro-Russian hacker groups are yet another example of the heightened and tense cyber threat landscape that EU and its Member States have observed. We strongly condemn this unacceptable behaviour in cyberspace and express solidarity with all countries that have fallen victim. We remain determined to address and investigate malicious cyber activities affecting international peace, security and stability, including the security of the European Union and its Member States, their democratic institutions, citizens, businesses, and civil society." READ MORE

RELATED ARTICLE:

The Record, Russian hacking risks 'spillover effects' and possible escalation, EU warns, 20 July 2022

Source: Europol

Date: 26 July 2022

Hit by ransomware? No More Ransom now offers 136 free tools to rescue your files

"Ransomware attacks have been growing in number and severity for years, with headlines focused on ransom demands that have climbed to amounts once unthinkable. While the data is alarming, it does not mean that you are helpless against the high-tech extortionists orchestrating these attacks. The No More Ransom initiative offers over a hundred free decryption tools to rescue your hostage files. Celebrating its sixth anniversary today, No More Ransom provides keys to unlocking encrypted files as well as information on how to avoid getting infected in the first place. Launched by Europol, the Dutch National Police (Politie) and IT security companies, the No More Ransom portal initially offered four tools for unlocking different types of ransomware and was available only in English. Six years later, No More Ransom offers 136 free tools for 165 ransomware variants, including Gandcrab, REvil/Sodinokibi, Maze/Egregor/Sekhmet and more. Over 188 partners from the public and private sector have joined the scheme, regularly providing new decryption tools for the latest strains of malicious software." READ MORE

Source: European Data Protection Supervisor

Date: 29 July 2022

Proposal to combat child sexual abuse online presents serious risks for fundamental rights

"The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) adopted a Joint Opinion on the Proposal for a Regulation to prevent and combat child sexual abuse. The Proposal aims to impose obligations related to detecting, reporting, removing and blocking known and new online child sexual abuse material (CSAM), as well as the solicitation of children, on providers of hosting services, interpersonal communication services, software application stores, internet access services and other relevant services. The EDPB and EDPS consider child sexual abuse as a particularly serious and heinous crime. Limitations to the rights to private life and data protection must, however, respect the essence of these fundamental rights and remain limited to what is strictly necessary and proportionate. The EDPB and EDPS consider that the Proposal, in its current form, may present more risks to individuals, and, by extension, to society at large, than to the criminals pursued for CSAM." READ MORE

Source: The Record

Date: 22 July 2022

Twitter investigating authenticity of 5.4 million accounts for sale on hacking forum

"Twitter said it is investigating the authenticity of a batch of information connected to 5.4 million accounts that is being sold on a hacking forum. First reported by RestorePrivacy, the hacker – going by the name "devil" – is offering email addresses and phone numbers connected to the accounts. The hacker claimed in the post on Breach Forums that the accounts range from "celebrities, companies, randoms, OGs, etc." Researchers immediately tied the post to a vulnerability in Twitter's platform that was discovered in January by a security researcher who reported the issue through the HackerOne site." READ MORE

Source: Reuters

Date: 27 July 2022

EU found evidence employee phones compromised with spyware -letter

"The European Union found evidence that smartphones used by some of its staff were compromised by an Israeli company's spy software, the bloc's top justice official said in a letter seen by Reuters. In a July 25 letter sent to European lawmaker Sophie in 't Veld, EU Justice Commissioner Didier Reynders said iPhone maker Apple had told him in 2021 that his iPhone had possibly been hacked using Pegasus, a tool developed and sold to government clients by Israeli surveillance firm NSO Group. The warning from Apple triggered the inspection of Reynders' personal and professional devices as well as other phones used by European Commission employees, the letter said." READ MORE

Source: Expansion

Date: 25 July 2022

Nueve detenidos por una ciberestafa de más 3 millones de euros

"Agentes de la Policía Nacional, en una operación conjunta con la Policía Nacional de Rumanía y Europol, han desarticulado una organización internacional que habría estafado más de 3 millones de euros mediante fraudes cometidos a través de internet. Nueve personas han sido detenidas, en España y Rumanía, por publicar en internet anuncios falsos de venta de vehículos de segunda mano y otros productos, en los que solicitaban un pago por adelantado y, una vez recibido, desaparecían sin dejar rastro, ha informado la Policía Nacional." READ MORE

Source: The Register

Date: 25 July 2022

Cyber-mercenaries for hire represent shifting criminal business model

"An emerging and fast-growing threat group is using a unique business model to offer cybercriminals a broad range of services that span from leaked databases and distributed denial-of-service (DDoS) attacks to hacking scripts and, in the future, potentially ransomware. The Atlas Intelligence Group – or AIG or Atlantis Cyber-Army – was first detected in May and initially appeared to be a run-of-the-mill data leakage gang, according to threat intelligence researchers at Cyberint. However, as a clearer picture of AIG emerged, it became obvious that the group's operations were anything but business as usual. As cybercrime becomes more profitable, with some groups bringing in hundreds of millions of dollars, threat groups have evolved to include business models that mirror those of many corporations, with everything from CEOs to HR departments to time-off policies for their employees. That was illustrated earlier this year by the information leaks of ransomware group Conti's operations." READ MORE

Source: BBC

Date: 22 July 2022

Cyber-attacks on Port of Los Angeles have doubled since pandemic

"Cyber-attacks on one of the world's busiest ports have nearly doubled since the start of the Covid pandemic. The number of monthly attacks targeting the Port of Los Angeles is now around 40 million, the port's executive director Gene Seroka told the BBC. Los Angeles is the busiest port in the western hemisphere, handling more than $250bn (£210bn) of cargo every year. […]The Port of Los Angeles Cyber Operations Security Centre, operating since 2015 is part of an overall network of FBI cyberwatch programs. In addition to that the Port of Los Angeles has invested millions of dollars in cyber-protection, developing one of the world's first Cyber Resilience Centres. "We must take every precaution against potential cyber-incidents, particularly those that could threaten or disrupt the flow of cargo," said Mr Seroka. The Cyber Resilience Centre provides enhanced intelligence gathering and heightened protection against cyber-threats within the maritime supply chain." READ MORE

Source: Diario de Valdivia

Date: 29 July 2022

Chile: Entró en vigencia la nueva Ley de Delitos Informáticos

"A nivel nacional fueron creadas las Brigadas del Cibercrimen y a nivel local, las denuncias por estos hechos son cursadas a través de la Brigada Investigadora de Delitos Económicos Valdivia, y en la provincia del Ranco, se reciben a través de la Brigada de Investigación Criminal La Unión. Lo anterior, luego de que hasta junio, las Brigadas del Cibercrimen, tenían como finalidad, investigar los delitos contemplados en la Ley Nº19.223 que "Tipifica figuras penales relativas a la informática" y aquellos en los cuales la tecnología es el medio para cometerlos. Sin embargo, a contar del 9 de junio de 2022 se establece la nueva normativa de los delitos informáticos en el país y los tipifica, con la nueva Ley N°21.459, derogando a la normativa anterior (Ley N°19.223). Además, adecua otras legislaciones afines para aplicar al Convenio de Budapest en aspectos como defraudación informática o acceso indebido a sistemas o datos." READ MORE

RELATED ARTICLE:

El Tipografo, Nueva Ley de Delitos Informáticos: PDI da a conocer sus alcances, 19 July 2022

Source: BBC

Date: 20 July 2022

US seizes stolen funds from suspected North Korean hackers

"The US Department of Justice has seized $500,000 (£417,000) worth of Bitcoin from suspected North Korean hackers. The hackers attacked healthcare providers with a new strain of ransomware, extorting the funds from several organisations. US authorities say they have already returned ransom payments to two hospital groups. The rare successful seizure comes as US authorities warn that North Korea is becoming a major ransomware threat. In a conference on Tuesday, Deputy Attorney General Lisa O. Monaco praised an unnamed Kansas hospital for alerting the FBI early about the ransomware attack. "Not only did this allow us to recover their ransom payment as well as a ransom paid by previously unknown victims, but we were also able to identify a previously unidentified ransomware strain," she said." READ MORE

RELATED ARTICLE:

Dark Reading, US Offers $10M Double-Reward for North Korea Cyberattacker Info, 27 July 2022

Source: Politico

Date: 28 July 2022

Justice Department investigating data breach of federal court system

"The Justice Department is investigating a data breach of the U.S. federal courts system dating to early 2020, a top official testified on Capitol Hill Thursday. Scary scenario for the judicial branch: House Judiciary Committee Chair Jerrold Nadler (D-N.Y.) told fellow lawmakers that "three hostile foreign actors" attacked the U.S. Courts' document filing system as part of a breach in early 2020 causing a "system security failure." The comments — at a committee hearing on oversight of the Justice Department's National Security Division — were the first public disclosure of the hack. Nadler said the committee learned in March about the "startling breadth and scope" of the breach, which was separate from the SolarWinds hack revealed in late 2020." READ MORE

Source: Swiss Info

Date: 20 July 2022

Ministerio de Educación de Costa Rica en alerta por amenaza cibernética

"El Ministerio de Educación Pública (MEP) de Costa Rica informó este miércoles que se encuentra bajo alerta tras una amenaza cibernética a sus sistemas, lo que ha obligado a desactivar los servicios y deshabilitar los servidores institucionales. El ente indicó en un comunicado de prensa que el día lunes recibió una alerta de amenaza cibernética a los sistemas del Ministerio, lo que motivó que la Dirección de Informática de Gestión activara el protocolo previsto, que incluye preventivamente deshabilitar los servidores institucionales. "De forma preventiva se procedió a deshabilitar los sistemas, de momento no se ha logrado determinar vulneración alguna, pero esto ha implicado que el día de hoy no haya acceso a las plataformas de consulta. En estos momentos el departamento de informática está tratando de habilitar los sistemas a la mayor brevedad", explicó en unas declaraciones distribuidas a los medios el director de Comunicación el Ministerio de Educación, Otto Vargas." READ MORE

Source: Reuters

Date: 20 July 2022

Limits on personal data gathering by Google, Facebook, others advance in U.S. House

"A U.S. House of Representatives committee approved on Wednesday a bill to create the first U.S. privacy law limiting personal information collected online by companies like Alphabet's Google and Meta's Facebook. The House Energy and Commerce Committee approved the bill by a margin of 53-2. It now goes to the House floor. A companion bill is before the Senate. Privacy legislation has been introduced regularly in Congress but failed amid fights over whether it would preempt state laws, which are sometimes stronger, or whether individuals would be allowed to sue in the case of privacy violations." READ MORE

Source: Graphic Online

Date: 25 July 2022

Ghana: Policy to create child-friendly internet in the offing

"More than a third of Ghanaian young people between 12-17 years have access to the internet, mostly using mobile phones. However, the greater use of the internet increasingly exposes children and young people to the dangers of all forms of abuse. A recent UNICEF Ghana report showed that many children had indicated that they have been treated in a hurtful way by someone else when using the internet. Boys, older children and those living in urban areas report upsetting incidents more often. Sexual content, hurtful comments, fraud or violence are among the things that children find upsetting." READ MORE

Source: Les Echos du Niger

Date: 21 July 2022

Cybersécurité au Niger: bientôt une stratégie nationale

"Face aux attaques cybercriminelles, le Niger envisage renforcer son cadre sécuritaire. Un avant-projet de stratégie nationale a été élaboré dans ce cadre et a été au cœur d'un atelier hier mercredi 20 juillet 2022 à Niamey. Le projet élaboré devrait concourir au renforcement de la sécurité des données des institutions publiques et privées mais aussi des personnes physiques souvent les plus exposées. « Ce n'est pas un privilège, elle s'impose à nous face aux enjeux du cyberespace. Elle est nécessaire pour notre pays de disposer d'une Stratégie Nationale de Cybersécurité. La définition d'une Stratégie nationale de Cybersécurité est une étape importante pour assurer la transformation numérique de la société nigérienne », a argumenté le ministre." READ MORE

Source: Council of Europe

Date: 13-15 July 2022

CyberSouth: Judicial Training Course on International Co-operation on Cybercrime and Electronic Evidence in Lebanon

"From 13 to 15 July 2022, the Cybercrime Programme Office of the Council of Europe (C-PROC), within the framework of the joint European Union – Council of Europe CyberSouth project and in co-operation with the Lebanese Ministry of Justice, organised a judicial training course on international co-operation for judges and prosecutors. […] The participants from the Lebanese institutions discussed on how to apply international provisions to the national context, reflecting on the diverse tools and channels offered by the Convention on Cybercrime Budapest Convention and its newly opened for signature Second Additional Protocol. Lebanon plans to introduce new provisions to facilitate international co-operation and is currently finalising a new draft law on data protection, which will improve safeguards on handling personal data, in compliance with international standards." READ MORE

Source: The New Times

Date: 18 July 2022

Kigali meet calls for tougher actions against cybercrime

"Law enforcement agencies must step up by enhancing measures to detect and prevent the cyber-attacks from the source, where investigation and prosecution can effectively take place, Justice Minister Emmanuel Ugirashebuja has said. He made the call while officiating the 9th Africa Working Group meeting on Cybercrime for heads of units, in Kigali that will last for one week. The meeting was co-organised by Rwanda Investigation Bureau (RIB) and Interpol. "Rwanda greatly appreciates Interpol's continued support in the fight against cybercrime and its effort in enabling African countries to engage in discussions with experts and learn from their experiences on diverse aspects of cybercrime," said Ugirashebuja." READ MORE

Source: Ghana Today

Date: 25 July 2022

Ghana: Communication Minister calls for collaboration to curb cybercrime

"The Minister for Communication and Digitalization, Mrs Ursula Owusu-Ekuful has charged the Cyber Security Agency (CSA) to build a resilient telecommunication system to detect cybercrime and safeguard the activities of consumers online. That, she said, would help create an enabling environment for the effective use of Information Communication Technology (ICT). The Minister gave this advice at the Consumer Forum on Telecommunications Services, in Kumasi." READ MORE

Source: The Diplomat

Date: 22 July 2022

Hong Kong's New Cybercrime Law Consultation

"This week the Cybercrime Subcommittee of the Law Reform Commission (LRC) in Hong Kong published a consultation paper on cybercrimes and related jurisdictional issues, setting in motion what will likely be a series of legislations of new laws and amendments in the reformed "patriots-ruled" territory under the People's Republic of China. The move should come as no surprise. After all, many other jurisdictions around the world have legislated cybercrime in various shapes and forms in recent years. As technology advances, news laws try to catch up. The LRC's Cybercrime Subcommittee actually commenced work back in January 2019, a full three-and-a-half years ago, to review Hong Kong's relevant laws, long considered to be grossly outdated." READ MORE

Source: ABC News

Date: 27 July 2022

Half of all Australians have been victims of tech abuse, landmark study reveals

"The first-known representative study of its kind — commissioned by Australia's National Research Organisation for Women's Safety (ANROWS) — has revealed half of all Australian adults have experienced technology-facilitated abuse at some point in their lives.That extraordinary figure includes a variety of issues and victims: from a man abusing a male colleague online to a stranger stalking someone on social media to an ex monitoring a former partner's movements via an app. The research — comprising an initial sample of more than 4,500 Australian adults — also highlights the deep impact that tech abuse can have on minority groups, and women in particular, who are far more likely to experience this at the hands of an intimate partner." READ MORE

Source: The Wall Street Journal

Date: July 2022

Moldova Plans Cyber Overhauls Amid War in Neighboring Ukraine

"Moldova is working to step up cyber defenses to protect its critical infrastructure from rising threats amid the war in neighboring Ukraine. Officials in the country of roughly three million people are planning overhauls to create basic cybersecurity rules and institutions. The plans include drafting new legislation in line with European Union guidelines, improving security in government offices and launching a new national computer emergency response team, or CERT, by the end of the year that would deal with cyberattacks on government and other essential services." READ MORE

Source: The Guardian

Date: 21 July 2022

UK cybersecurity chiefs back plan to scan phones for child abuse images

"Tech companies should move ahead with controversial technology that scans for child abuse imagery on users' phones, the technical heads of GCHQ and the UK's National Cybersecurity Centre have said. So-called "client-side scanning" would involve service providers such as Facebook or Apple building software that monitors communications for suspicious activity without needing to share the contents of messages with a centralised server. Ian Levy, the NCSC's technical director, and Crispin Robinson, the technical director of cryptanalysis – codebreaking – at GCHQ, said the technology could protect children and privacy at the same time. "We've found no reason why client-side scanning techniques cannot be implemented safely in many of the situations one will encounter," they wrote in a discussion paper published on Thursday, which the pair said was "not government policy"." READ MORE

Source: The Register

Date: 28 July 2022

Suspected radiation alert saboteurs cuffed by cops after sensors disabled

"Spain's national police say they have arrested two former government workers suspected of breaking into the computer network of the country's radioactivity alert system (RAR) and disabling more than a third of its sensors. The intrusion happened between March and June 2021, and the two suspects worked for a company contracted by Spain's General Directorate of Civil Protection and Emergencies (DGPCE), according to officers. Investigators searched two homes and one company in Madrid and San Agustín de Guadalix, and said they found "numerous computer and communications devices related to the facts investigated." The year-long probe eventually traced the cyberattack to a computer "in the public-use network of a well-known establishment of hospitality in the center of Madrid," which the cops said allowed them to identify the perpetrators." READ MORE

Source: Bleeping Computer

Date: 19 July 2022

Belgium says Chinese hackers attacked its Ministry of Defense

"The Minister for Foreign Affairs of Belgium says multiple Chinese state-backed threat groups targeted the country's defense and interior ministries. "Belgium exposes malicious cyber activities that significantly affected our sovereignty, democracy, security and society at large by targeting the FPS Interior and the Belgian Defence," the foreign minister said. "Belgium assesses these malicious cyber activities to have been undertaken by Chinese Advanced Persistent Threats (APT)." READ MORE

Source: Infosecurity Magazine

Date: 9 July 2022

UK Seizes Nearly $27m in Crypto-Assets

"The UK's National Crime Agency (NCA) seized millions of pounds' worth of cryptocurrency last year as part of its efforts to crack down on money laundering and serious and organized crime (SOC). The NCA, which is the UK agency dedicated to tackling SOC, revealed in its latest annual report that during the period April 1 2021 to March 31 2022 it confiscated $26.9m in cryptocurrency assets, at prices calculated in March this year. Six years later, No More Ransom offers 136 free tools for 165 ransomware variants, including Gandcrab, REvil/Sodinokibi, Maze/Egregor/Sekhmet and more. Over 188 partners from the public and private sector have joined the scheme, regularly providing new decryption tools for the latest strains of malicious software. To date, the scheme has so far helped over 1.5 million people successfully decrypt their devices without needing to pay the criminals. The portal is available in 37 languages in order to better assist victims of ransomware across the globe." READ MORE

Source: Euronews

Date: 19 July 2022

Widespread cyberattack blocks government and public websites in Albania

"Albanian authorities are investigating after the official government website was shut down on Monday after a major cyberattack. The "wide and complex" attack began on Friday and targeted government infrastructure and other public online services, according to a statement. It began as a ransomware attack as hackers tried to hit critical systems and render them functionless, the government added. The statement said the "method used by the hackers was identical with the last year's attacks seen in the international cyberspace," mentioning those in Belgium, Germany, Lithuania, Malta, the Netherlands and Ukraine. Those behind the cyberattack have not been identified. Albanian authorities are investigating after the official government website was shut down on Monday after a major cyberattack." READ MORE

RELATED ARTICLE:

Balkan Insight, Albania Blames 'Massive Cyber Attack' as Govt Servers go Down, 18 July 2022

Source: Reuters

Date: 28 July 2022

Russia fines WhatsApp, Snap and others for storing user data abroad

"A Russian court on Thursday fined Meta Platforms Inc's (META.O) WhatsApp messenger, Snapchat owner Snap Inc (SNAP.N) and other foreign firms for their alleged refusal to store the data of Russian users domestically. Moscow has clashed with Big Tech over content, censorship, data and local representation in disputes that have escalated since Russia sent its armed forces into Ukraine on Feb. 24. Moscow's Tagansky District Court fined WhatsApp 18 million roubles ($301,255) for a repeat offence after it incurred a 4 million rouble penalty last August. WhatsApp's fine exceeded the 15 million rouble penalty handed to Alphabet Inc's (GOOGL.O) Google for a repeat infringement last month. The court fined Tinder owner Match Group (MTCH.O) 2 million roubles, Snap and Hotels.com, owned by Expedia Group Inc (EXPE.O), 1 million roubles, and music streaming service Spotify (SPOT.N) 500,000 roubles." READ MORE

Latest reports

- Beta news, The evolution of botnets and DDoS attacks (betanews.com). July 2022
- JV Tech, Cybersécurité : la France est 4e des pays à l'origine des menaces informatiques, 19 July 2022
- HP, The Evolution of Cybercrime: Why the Dark Web is Supercharging the Threat Landscape and How to Fight Back, 21 July 2022
- Ahval, Turkish government agency collecting every activity of Internet users – report, 21 July 2022
- EUROJUST, Artificial intelligence supporting cross-border cooperation in criminal justice, 22 July 2022
- ZD NET, How to find and remove spyware from your phone, 22 July 2022
- Europol, No More Ransom infographic, 26 July 2022
- Bleeping computer, DDoS Attack Trends in 2022: Ultrashort, Powerful, Multivector Attacks, 27 July 2022
- IT World Canada, Average cost of a data breach to Canadian firms studied hit $7 million, says IBM, 27 July 2022
- ENISA, ENISA Threat Landscape for Ransomware Attacks, 29 July 2022
- Revista Seguridad 360, Estrategia de ciberseguridad en Argentina, 22 July 2022
- The European Sting, Nearly half of businesses are being hit by economic crime, with cybercrime the gravest threat. What can they do about it? 27 July 202

Upcoming events

- July-August, C-PROC *(online)*, Finalization of the translation of the Electronic Evidence Guide v3.0 into Albanian, Macedonian, Serbian and Turkish, iPROCEEDS-2
- July-August, C-PROC *(online)*, Legislation study report on national legislation of Moldova in light of the Second Additional Protocol, CyberEast
- July-August, C-PROC *(online)*, EaP legislation study on search, seizure and confiscation of cybercrime proceeds and prevention of money laundering, CyberEast
- July-August, C-PROC *(online)*, EaP research study on Guidelines on the prevention and control of online fraud and criminal money flows applicable in EaP region, working with publicly available
- sources and inquiries with the region's countries, CyberEast
- 1-15 August, C-PROC, (*online*) Further development of the cyberviolence resource, Octopus project
- 2 August, CPROC/CoE Office in Rabat, *(online)*: finalisation of the translation of the HELP course on cybercrime in Arabic, CyberSouth
- 4 August, CPROC/EU CyberNet, *(online),* EU CyberNet Club: Budapest Convention, GLACY+
- 5 August, PILON/CPROC, *(online),* PILON/CoE co-branded Regional Webinar on cybercrime legislation, Pacific, GLACY+
- 8 August, T-CY/Faculdad de Derecho, Universidad de Buenos Aires, Argentina, Jornada @UBA Cibercrimen
- 8-9 August, T-CY/Argentina, Primera Conferencia Cumbre sobre Asuntos Cibernéticos
- 10-12 August, T-CY visit to Uruguay, Octopus project
- 13-15 August, CPROC/SRI LANKA, *(online)*, Refresher on the Budapest Convention, on Cybercrime and on electronic evidence for Trainer Justices of Supreme Court of Sri Lanka and courts of appeal, GLACY+

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