Council of the EU

PRESS
EN

PRESS RELEASE
568/24
24/06/2024

# Cyber-attacks: six persons added to EU sanctions list for malicious cyber activities against EU member states and Ukraine

The Council today approved additional restrictive measures against **six persons** involved in cyber-attacks affecting information systems relating to critical infrastructure, critical state functions, the storage or processing of classified information and government emergency response teams in EU member states. For the first time, restrictive measures are being taken against cybercriminal actors that use ransomware campaigns against essential services, such as health and banking.

The new listings include two members of the '**Callisto group**', Ruslan **Peretyatko** and Andrey **Korinets**. The 'Callisto group' is a group of Russian intelligence officers conducting cyber operations against EU member states and third countries through sustained phishing campaigns intended to steal sensitive data in critical state functions, including defence and external relations.

The EU also targeted Oleksandr **Sklianko** and Mykola **Chernykh** of the '**Armageddon hacker group**', a group supported by the Federal Security Service (FSB) of the Russian Federation that carried out various cyber-attacks with a significant impact on the governments of EU member states and Ukraine, including by using phishing emails and malware campaigns.

In addition, Mikhail **Tsarev** and Maksim **Galochkin**, key players in the deployment of the malwares 'Conti' and 'Trickbot' and involved in 'Wizard Spider', are also sanctioned. Trickbot is a malicious spyware program, created and developed by the threat group 'Wizard Spider', which has conducted ransomware campaigns in a variety of sectors, including essential services such as health and banking, and is therefore responsible for significant economic damage in the European Union.

The EU horizontal cyber sanctions regime currently applies to **14 individuals** and **four entities**, and includes an **asset freeze** and a **travel ban**. Additionally, EU persons and entities are **forbidden from making funds available** to those listed.

With these new listings, the EU and its member states reaffirm their willingness to step up efforts to provide a stronger and more sustained response to persistent malicious cyber activities targeting the EU, its member states and partners. This is in line with joint efforts with our international partners, such as the UK and the US, to disrupt and respond to cyber crime. The EU remains committed to a global, open, and secure cyberspace and, reiterate the need to strengthen international cooperation to promote the rules-based order in this area.

*The relevant legal acts have been published in the Official Journal of the European Union.*

## Background

In June 2017, the EU established a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the "Cyber Diplomacy Toolbox"). The framework allows the EU and its member states to use all CFSP measures, including restrictive measures if necessary, to prevent, discourage, deter and respond to malicious cyber activities targeting the integrity and security of the EU and its member states.

The EU framework for restrictive measures against cyber-attacks threatening the EU and its member states was set up in May 2019.

On the 21st of May, 2024 the Council approved conclusions on the future of cybersecurity aiming to provide guidance and setting the principles towards building a more cyber secure and more resilient EU.

The European Union and its member states, together with its international partners, have strongly condemned the malicious cyber activity conducted by the Russian Federation. This was also the case in 2020 on the attack against Ukraine, which targeted the satellite KA-SAT network, owned by Viasat. Russia has continued their pattern of irresponsible behaviour in cyberspace, which also formed an integral part of its illegal and unjustified invasion of Ukraine.

The EU will continue to strengthen its cooperation in particular with Ukraine to advance international security and stability in

cyberspace, increase global resilience and to raise awareness on cyber threats and malicious cyber activities.

- Council Decision (CFSP) 2024/1779 of 24 June 2024 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyberattacks threatening the Union or its Member States (including a list of sanctioned individuals)
- Cybersecurity: Council approves conclusions for a more cyber secure and resilient Union (press Release 21 May, 2024)
- Cybersecurity: How the EU tackles Cyber Threads (background information)
- Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (consolidated text dated 23 November 2023)

**Press office - General Secretariat of the Council of the EU**
Rue de la Loi 175 - B-1048 BRUSSELS - Tel.: +32 (0)2 281 6319
press@consilium.europa.eu - www.consilium.europa.eu/press