NEWS

Ransomware gangs cut off from EUR 336 million ‘AudiA6’ crypto laundering pipeline

Europol analysis links the criminal service to over 15 international cybercrime investigations

Publish date11 Jun 2026

An international law enforcement operation has dismantled one of the cryptocurrency laundering services most trusted by ransomware gangs and cybercriminal networks, cutting off a key financial pipeline used to wash hundreds of millions in illicit profits.

The service, known as ‘AudiA6’, is suspected of laundering more than EUR 336 million between 2022 and 2025. Investigators believe the platform became a central hub for ransomware actors and cybercriminals seeking to cash out stolen digital assets while hiding the money trail from authorities.

The suspects behind ‘AudiA6’ are also believed to have administered the dark web cybercrime forum ‘Dark2Web’, a criminal marketplace used to advertise illicit services and connect cybercriminal actors worldwide.

The parallel investigations were conducted by the United States Secret Service and the IRS Criminal Investigation on one side, and the Polish Police on the other, together with EU Member States and other international law enforcement partners, with the support of Europol and Eurojust.

On 10 June, a coordinated action took place, during which:

- 2 alleged administrators of Ukrainian and Russian nationality were arrested in Georgia
- 3 properties were searched
- 25 domains were taken down and more than 30 servers were seized
- Over 80 vehicles and multiple properties were seized in Georgia
- EUR 692 000 in cryptocurrency was frozen and over EUR 86 000 in cryptocurrency seized
- Telegram accounts used by the network were blocked

The clear web and dark web websites of the ‘AudiA6’ service and the ‘Dark2Web’ cybercrime forum were replaced with a law enforcement seizure banner

The action built on earlier enforcement action carried out by the Polish Police which led to the arrest on 15 September 2025 of a Ukrainian national involved in money laundering activities connected to the AudiA6 group. During the searches, electronic devices belonging to the suspect were seized. The forensic examination of these devices enabled investigators to identify additional individuals involved in the money laundering operation.

A crypto cleaning service for cybercriminals

Investigators uncovered what they describe as an industrial-scale cryptocurrency laundering operation built around thousands of fraudulent exchange accounts opened using stolen or purchased identities. Analysis conducted by Europol linked the criminal service to more than 15 investigations worldwide involving ransomware attacks and large-scale cryptocurrency theft.

Marketed on underground cybercrime forums as a professional cryptocurrency mixing service, ‘AudiA6’ promised criminals anonymity and speed.

After establishing contact with the criminal service through private messaging platforms, customers transferred stolen cryptocurrency to wallets controlled by the criminal group and, within around an hour, received “cleaned” funds back through a complex chain of transactions designed to conceal the origin of the money. The operators charged commissions of between 3 and 10 percent.

More than 6 000 Know Your Customer (KYC) records linked to money mule accounts were identified during the investigation. Many of the mule accounts were connected to Russian-speaking intermediaries recruited specifically to help move criminal proceeds through cryptocurrency exchanges.

The group used both commercial email providers and email addresses linked to domains under their control to register money mule accounts with various cryptocurrency exchanges. These domains are being made public to help cryptocurrency exchanges identify and block accounts associated with this money laundering service:

designli.pictures

pheontx.eu

smplfy.in

sumato-soft.org

technobrains.dev

lett.email

trayo.app

deliverly.top

inboxly.top

postfast.eu

postino.click

inboxally.agency

mailora.eu

postify.email

quix.express

flowcomm.click

qube.black

deliverlett.com

lettermail.eu

European activities

Europol’s European Cybercrime Centre analysed the criminal money trail behind the laundering service. Europol’s cybercrime and cryptocurrency experts traced illicit crypto flows, helped map the laundering infrastructure used to move criminal profits across borders and supported European law enforcement authorities with intelligence development ahead of the final phase of the investigation.

During the action day, Europol assisted with the rapid exchange of operational intelligence between authorities as arrests were carried out, servers taken down and cryptocurrency assets seized simultaneously in multiple countries.

The Joint Cybercrime Action Taskforce (J-CAT) hosted at Europol also supported coordination, liaison, and deconfliction efforts with national authorities.

Eurojust supported the judicial authorities throughout the investigation. Several coordination meetings at the Agency were held to prepare for the execution of judicial measures in France, Poland, Georgia and Iceland. Additionally, Eurojust ensured that Mutual Legal Assistance requests were executed in several jurisdictions.

Participating authorities

Australia: Australian Federal Police

Canada: Royal Canadian Mounted Police (RCMP)

France: Public Prosecutor’s Office Paris Cybercrime Unit ; National Gendarmerie (Gendarmerie Nationale - Unité nationale cyber)

Georgia: Investigation Department of the Office of the Prosecutor General of Georgia

Germany: Federal Criminal Police Office (Bundeskriminalamt), State Criminal Police Office of North Rhine – Westphalia (Landeskriminalamt Nordrhein-Westfalen)

Iceland: Director of Public Prosecutions; Reykjavík Metropolitan Police

Japan: National Police Agency of Japan

Poland: Regional Prosecutor’s Office in Łódź, Branch in Łódź of the Central Cybercrime Bureau

Switzerland: Federal Office of Police (fedpol)

United Kingdom: National Crime Agency (NCA)

United States: United States Secret Service (USSS), IRS Criminal Investigation (IRS-CI), Federal Deposit Insurance Corporation Office of Inspector General (FDIC OIG), Homeland Security Investigations (HSI)

The professionalisation of crypto laundering

The investigation reflects a growing threat identified in Europol’s latest Internet Organised Crime Threat Assessment (IOCTA): the rise of industrial-scale cryptocurrency laundering services powering the cybercrime economy.

Ransomware groups and cybercriminal networks are increasingly relying on chain-hopping, decentralised exchanges and “mixer-as-a-service” platforms to move illicit cryptocurrency across multiple blockchains within minutes, helping criminal profits disappear into the digital underground.

The report also warns of the growing use of fraudulent exchange accounts, mule wallets and privacy-focused tools designed to conceal criminal money flows and evade anti-money laundering controls - turning cryptocurrency laundering into a core service of the cybercrime ecosystem.

To explore these evolving threats further, Europol is organising a webinar series dedicated to cybercrime trends. One of the upcoming episodes, taking place on 30 June 2026, will examine the growing professionalisation of cybercrime services, including ransomware-as-a-service and cryptocurrency laundering techniques used to conceal criminal profits. Europol experts

will also discuss the increasing overlap between hybrid actors and cybercriminal networks. Registration for the webinar is open.

Email Alerts

Subscribe to receive an email when we publish content in the following categories.

Already a subscriber? Manage your subscription.

Metadata

Crime areas:

Cyber-attacks

Services:

Operational coordination Operational support Information exchange

Intelligence

Document type:

Press Release/News

Article type:

Press Release

Participating Countries:

Australia Canada France Georgia Germany Iceland Japan

Poland Switzerland United Kingdom United States

Entities:

European Cybercrime Centre (EC3)

Operations:

Other

Organisations:

Eurojust