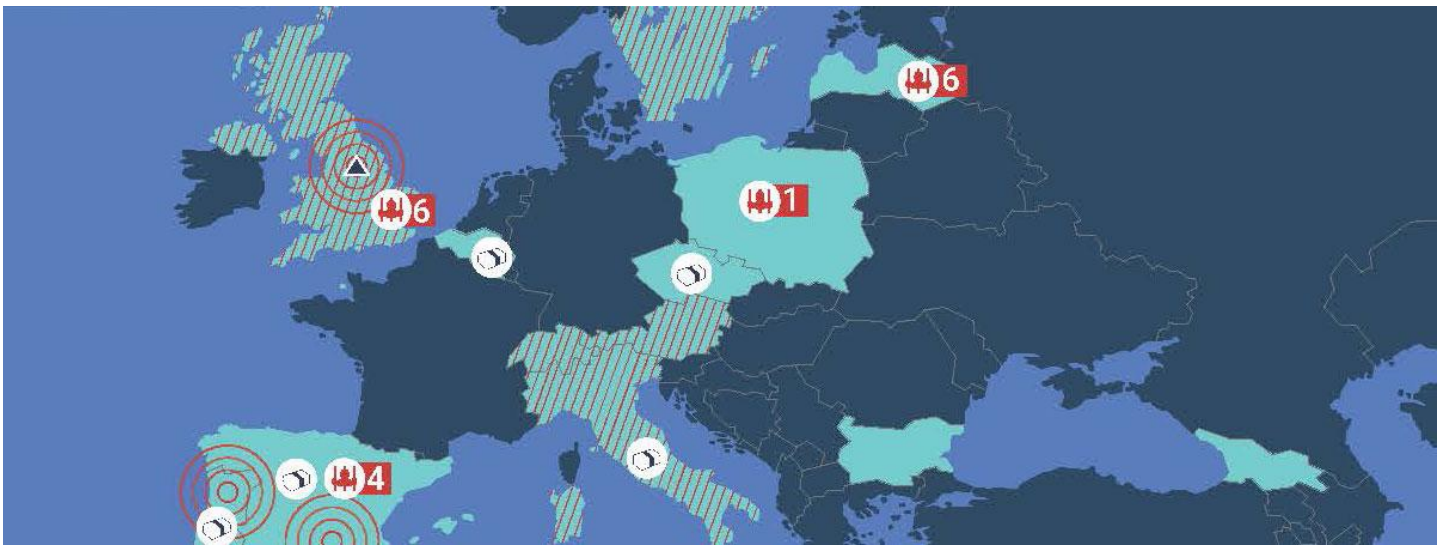
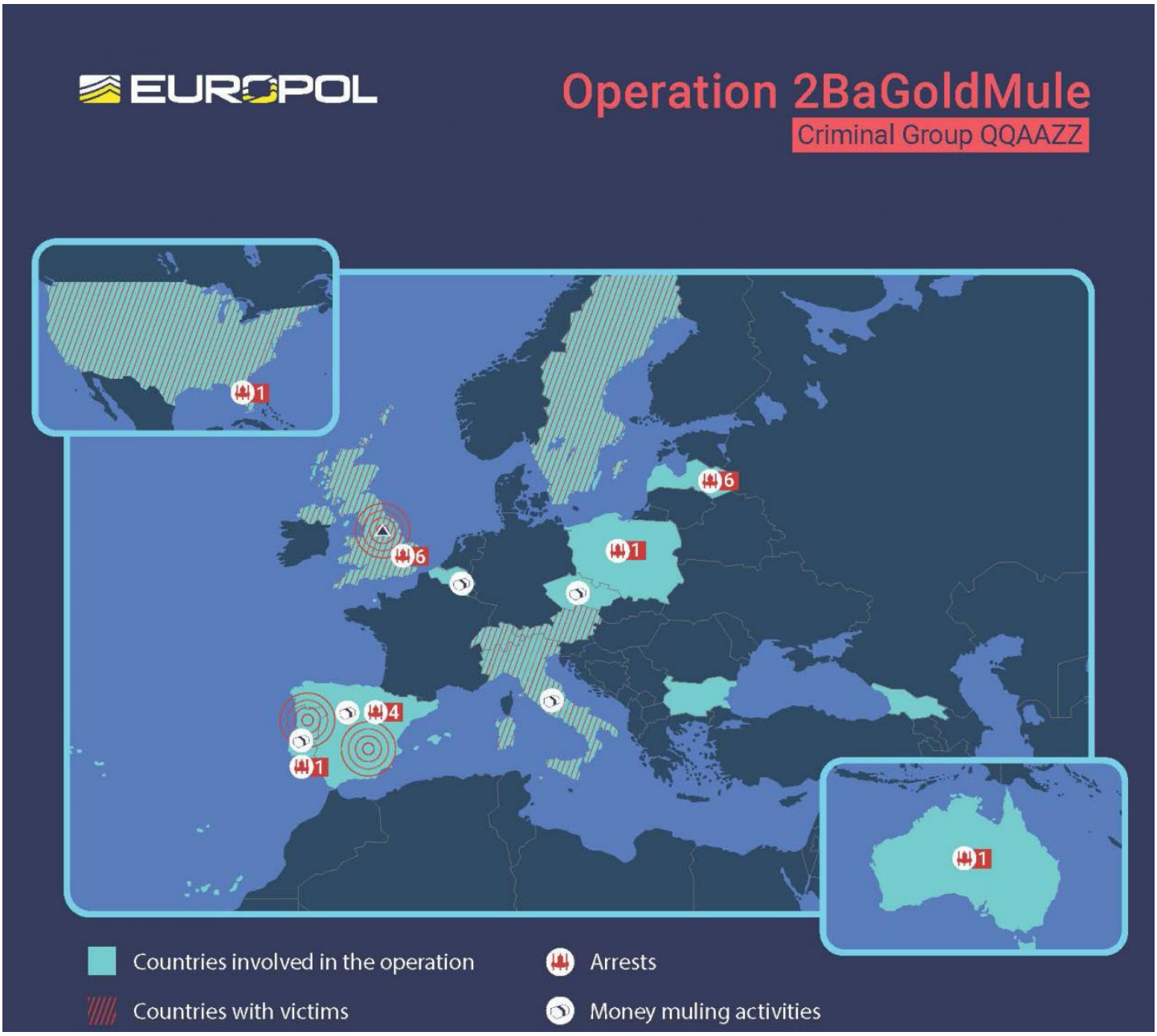
# 20 ARRESTS IN QQAAZZ MULTI-MILLION MONEY LAUNDERING CASE

15 Oct 2020

Press Release




An unprecedented international law enforcement operation involving 16 countries has resulted in the arrest of 20 individuals suspected of belonging to the QQAAZZ criminal network which attempted to launder tens of millions of euros on behalf of the world's foremost cybercriminals.

Some 40 house searches were carried out in Latvia, Bulgaria, the United Kingdom, Spain and Italy, with criminal proceedings initiated against those arrested by the United States, Portugal, the United Kingdom and Spain. The largest number of searches in the case were carried out in Latvia in operations led by the Latvian State Police (Latvijas Valsts Policija). Bitcoin mining equipment was also seized in Bulgaria.

This international sweep follows a complex investigation led by the Portuguese Judicial Police (Polícia Judiciária) together with the United States Attorney Office for the Western District of Pennsylvania and the FBI's Pittsburgh Field Office, alongside the Spanish National Police (Policia Nacional) and the regional Catalan police (Mossos D'esquadra) and law enforcement authorities from the United Kingdom, Latvia, Bulgaria, Georgia, Italy, Germany, Switzerland, Poland, Czech Republic, Australia, Sweden, Austria and Belgium with coordination efforts led by Europol.

## HOW THE QQAAZZ NETWORK CLEANED DIRTY MONEY

Criminal indictments returned by federal grand juries in Pittsburgh, United States, set forth allegations of how this criminal network operated. It is estimated that the QQAAZZ network laundered, or attempted to launder, tens of millions of euros in stolen funds since 2016.

Comprised of several layers of members mainly from Latvia, Georgia, Bulgaria, Romania, and Belgium, the QQAAZZ network opened and maintained hundreds of corporate and personal bank accounts at financial institutions throughout the world to receive money from cybercriminals who stole it from accounts of victims. The funds were then transferred to other QQAAZZ-controlled bank accounts and sometimes converted to cryptocurrency using 'tumbling' services designed to hide the original source of the funds. After taking a fee of up to 50-percent, QQAAZZ returned the balance of the stolen funds to their cybercriminal clientele.

The QQAAZZ members secured these bank accounts by using both legitimate and fraudulent Polish and Bulgarian identification documents to create and register dozens of shell companies which conducted no legitimate business activity. Using these registration documents, the QQAAZZ members then opened corporate bank accounts in the names of the shell companies at numerous financial institutions within each country, thereby generating hundreds of QQAAZZ-controlled bank accounts available to receive stolen funds from cyber thieves.

QQAAZZ advertised its services as a "global, complicit bank drops service" on Russian-speaking online cybercriminal forums where cybercriminals gather to offer or seek specialised skills or services needed to engage in a variety of cybercriminal activities. The criminal gangs behind some of the world's most harmful malware families (e.g.: Dridex, Trickbot, GozNym, etc.) feature among those having benefited from the services provided by QQAAZZ.

## INTERNATIONAL POLICE COOPERATION

International police cooperation coordinated by Europol was central in bringing the perpetrators to justice who were all located in different geographical locations around the world.

Europol's European Cybercrime Centre (EC3) hosted operational meetings, provided digital forensic support and facilitated the information exchange in the framework of the Joint Cybercrime Action Taskforce (J-CAT) hosted at Europol's headquarters in The Hague. Europol specialists were also deployed to Latvia and the United Kingdom to support the local authorities during the action days. The National Member for Portugal at Eurojust took part in a number of

operational meetings.

> Edvardas Šileris, Head of Europol's European Cybercrime Centre, said: "Cybercriminals are constantly exploring new possibilities to abuse technology and financial frameworks to victimise millions of users in a moment from anywhere in the world. Today's operation shows how through a proper law enforcement international coordination we can turn the table on these criminals and bring them to justice."

> Carlos Cabreiro, Director of the National Unit for Fighting Cybercrime and Technological Crime of the Polícia Judiciária, said: "Operation 2BaGoldMule has been a highly significant operation involving international law enforcement and prosecutors to tackle top-level cybercriminals who have laundered millions of euros for the world's foremost criminals. This operation has shown that through this cooperation we can collectively tackle the global nature of cybercrime. This is the only way forward."

> Scott W. Brady, United States Attorney for the Western District of Pennsylvania, said: "Cybercrime victimizes individuals and companies all over the world, so our work to identify and disrupt cybercriminals requires global collaboration. For the past several years, law enforcement from 16 countries has been conducting coordinated investigations of this criminal gang, and now parallel prosecutions will commence in the U.S., Portugal, United Kingdom and Spain. As this case demonstrates, we will be relentless in our pursuit of cybercriminals regardless of where they reside."

> Michael Christman, FBI Pittsburgh Special Agent in Charge, said: "This was an extensive investigation that had implications around the world. Partnerships are essential, as no one agency can combat cybercrime alone. This case highlights the FBI's strategy to target and dismantle the most significant cybercriminal enterprises through a global task force approach. I can assure everyone that the FBI and our partners will continue to work tirelessly to combat these cyber threats."

DOWNLOAD THE INFOGRAPHIC

EMPACT

In 2010 the European Union set up a four-year Policy Cycle to ensure greater continuity in the fight against serious international and organised crime. In 2017 the Council of the EU decided to continue the EU Policy Cycle for the 2018 - 2021 period. It aims to tackle the most significant threats posed by organised and serious international crime to the EU. This is achieved by improving and strengthening cooperation between the relevant services of EU Member States, institutions and agencies, as well as non-EU countries and organisations, including the private sector where relevant. Cybercrime is one of the priorities of the Policy Cycle.

| | |
|---|---|
| CRIME AREAS | Cybercrime |
| TARGET GROUPS | General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other |
| ENTITIES | European Cybercrime Center (EC3) |
| SUPPORT & SERVICES | Operational coordination • Information exchange |

**Source URL:** https://www.europol.europa.eu/newsroom/news/20-arrests-in-qqaazz-multi-million-money-laundering-case