

Officials Announce International Operation Targeting Transnational Criminal Organization QQAAZZ that Provided Money Laundering Services to High-Level Cybercriminals

 justice.gov/opa/pr/officials-announce-international-operation-targeting-transnational-criminal-organization

October 15, 2020



Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Thursday, October 15, 2020

U.S. Victims of Various Cybercriminal Malware Schemes throughout the United States Had Stolen Multi-Million Dollar Funds Laundered by QQAAZZ

Fourteen members of the transnational criminal organization, QQAAZZ, were charged by a federal grand jury in the Western District of Pennsylvania in an indictment unsealed today. A related indictment unsealed in October 2019 charged five members of QQAAZZ. One additional conspirator, a Russian national, was arrested by criminal complaint in late March 2020 while visiting the United States, bringing the total number of charged defendants to 20. Acting Assistant Attorney General Brian C. Rabbitt of the U.S. Department of Justice's Criminal Division and U.S. Attorney Scott W. Brady for the Western District of Pennsylvania, made the announcement today.

The QQAazz members, acting in concert with cybercriminals across the world, are accused of conspiring to launder money stolen from victims of computer fraud in the United States and elsewhere. More than 40 house searches were conducted in Latvia, Bulgaria, the United Kingdom, Spain and Italy, with criminal prosecutions initiated in the United States, Portugal, Spain and the United Kingdom. The largest number of searches and arrests were carried out in Latvia by the Latvian State Police (*Latvijas Valsts Policija*), and an extensive bitcoin mining operation associated with the group was seized in Bulgaria. Today's announcement is in coordination with announcements by Europol and several law enforcement agencies across Europe who collaborated with the United States to develop parallel investigations and prosecutions of the QQAazz members in their own countries.

"Today's charges, brought in coordination with our European law enforcement partners, reflect the Criminal Division's steadfast efforts to work with authorities worldwide to protect the public from fraudsters and the money launderers who help them hide their stolen money," said Acting Assistant Attorney General Brian C. Rabbitt. "Our message to money laundering organizations like QQAazz is simple: international borders will not stop the dedicated efforts of law enforcement across the globe to bring you to justice. In addition to the Criminal Division team, I would like to recognize the outstanding efforts of the team led by U.S. Attorney Scott Brady, FBI Pittsburgh, and our European partners."

"Cybercrime victimizes individuals and companies all over the world, so our work to identify and disrupt cybercriminals requires global collaboration," said U.S. Attorney Scott W. Brady for the Western District of Pennsylvania. "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 United States, Portugal, United Kingdom and Spain. As this case demonstrates, we will be relentless in our pursuit of cybercriminals regardless of where they reside."

"This was an extensive investigation that had implications around the world," said FBI Pittsburgh Special Agent in Charge Michael Christman. "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."

"Cybercriminals are constantly exploring new possibilities to abuse technology and financial frameworks to victimize millions of users in a moment from anywhere in the world," said Fernando Ruiz, Head of Europol's European Cybercrime Centre. "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."

The indictment alleges that the QQAazz network laundered, or attempted to launder, tens of millions of dollars' worth of stolen funds from victims of cybercrimes since 2016.

Comprised of several layers of members from Latvia, Georgia, Bulgaria, Romania, and Belgium, among other countries, 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 bank 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 40 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 around the world, 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 specialized 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.) are among those cybercriminal groups that benefited from the services provided by QQAAZZ.

The 14 defendants named in the indictment unsealed today are:

1. Nika Nazarovi, aka “Nika Utiashvili,” aka “Mihail Atansov,” aka “Stefan Trifonov Zhelyazkov,” 32, of Georgia;
2. Martins Ignatjevs, aka “Yordan Angelov Stoyanov,” aka “Aleksander Tihomirov,” aka “Svetlin Iliyanov Asenov,” 33, of Latvia;
3. Aleksandre Kobiashvili, aka “Antonios Nastas,” aka “Ognyan Krasimirov Trifonov,” 32, of Georgia;
4. Dmitrijs Kuzminovs, aka “Parush Gospodinov Genchev,” 35, of Latvia;
5. Valentins Sevecs, aka “Marek Jaswilko,” aka “Rafal Szczytko,” 32, of Latvia;
6. Dmitrijs Slapins, 35, of Latvia;
7. Armens Vecels, 24, of Latvia;
8. Artiom Capacli, 31, of Bulgaria;
9. Ion Cebanu, 26, of Romania;
10. Tomass Trescinkas, 25, of Latvia;
11. Ruslans Sarapovs, 19, of Latvia;
12. Silvestrs Tamenieks, 21, of Latvia;
13. Abdelhak Hamdaoui, 48, of Belgium; and
14. Petar Iliev, 37, of Bulgaria.

The five defendants charged in the indictment unsealed in October 2019 are:

1. Aleksejs Trofimovics, aka “Aleksejs Trofimovich,” aka “Alexey Trofimovich,” aka “Aleko Stoyanov Angelov,” 24, of Latvia;
2. Ruslans Nikitenko, aka “Krzysztof Wojciech Lewko,” aka “Milen Nikolchev Nikolov,” aka “Rafal Zimnoch,” 41, of Latvia;
3. Arturs Zaharevics, aka “Piotr Ginelli,” aka “Arkadiusz Szuberski,” 33, of Latvia;
4. Deniss Ruseckis, aka “Denis Rusetsky,” aka “Sevdelin Sevdalinov Atanasov,” 24, of Latvia; and
5. Deinis Gorenko, 25, of Latvia.

The Russian national charged by criminal complaint and arrested in late March 2020 while visiting the United States is Maksim Boiko, aka “Maxim Boyko” aka “gangass,” 30, of Russia.

The U.S. victims who had funds stolen, or attempted to be stolen, from their online bank accounts (including from banks headquartered in Pittsburgh, Pennsylvania) and destined for QAAZZ-controlled bank accounts overseas include:

- a technology company in Windsor, Connecticut;
- a Jewish Orthodox Synagogue in Brooklyn, New York;
- a medical device manufacturer in York, Pennsylvania;
- an individual in Montclair, New Jersey;
- an architecture firm in Miami, Florida;
- an individual in Acworth, Georgia;
- an automotive parts manufacturer in Livonia, Michigan;
- a homebuilder in Skokie, Illinois;
- an individual in Carrollton, Texas; and
- an individual in Villa Park, California.

Acting Assistant Attorney General Rabbitt and U.S. Attorney Brady praised the outstanding investigative work of the FBI’s Pittsburgh Field Office and their law enforcement partners from Portugal, Spain, the United Kingdom, Latvia, Bulgaria, Georgia, Italy, Switzerland, Poland, Czech Republic, Australia, Sweden, Austria, Germany and Belgium. Acting Assistant Attorney General Rabbitt and U.S. Attorney Brady also thanked Europol in The Hague, Netherlands for coordinating the investigative efforts of the law enforcement agencies from the 15 participating countries. The Justice Department’s Office of International Affairs of the Department’s Criminal Division provided significant assistance by coordinating requests to foreign countries for searches, arrests, extraditions and evidence sharing. Assistance was also provided by the National Cyber-Forensics and Training Alliance (NCFTA) in Pittsburgh.

The case is being prosecuted by Assistant U.S. Attorney Charles A. “Tod” Eberle, Chief of the National Security and Cybercrime Section for the Western District of Pennsylvania, Assistant U.S. Attorney Brian Czarnecki of the Western District of Pennsylvania, and Trial

Attorney Michael Parker of the Money Laundering and Asset Recovery Section of the U.S. Department of Justice's Criminal Division.

An indictment is an accusation. A defendant is presumed innocent unless and until proven guilty.