Inside Operation Destabilise: How a ransomware investigation linked Russian money laundering and street-level drug dealing

By Alexander Martin

Published: 2024-12-23 · Archived: 2026-04-06 00:28:28 UTC

Earlier this month, the United Kingdom's National Crime Agency (NCA) unveiled the most complex investigation that staff can remember. Over nearly four years, Operation Destabilise involved almost everyone at the agency.

What those staff uncovered was unprecedented for law enforcement: the complete financial chain connecting street-level drug dealing to the multibillion-dollar money-laundering operations that underpin criminal activities on a global scale.

Based on interviews with NCA investigators, this is the story of how pulling at the thread of a ransomware group's extortion funds ended up unravelling a Russian-speaking money-laundering network used by transnational drug traffickers, cybercriminals, Moscow elites evading sanctions and even the Kremlin's espionage operations. Two investigators asked to remain anonymous to speak freely about the operation.

It begins during 2021. By the middle of that year, ransomware attacks on Colonial Pipeline and the software company Kaseya had firmly established the scale of the threat in the minds of the investigators. The cyber team at the NCA was digging around the blockchain — the transparent ledger that underpins most crypto asset technologies — to track payments linked to the Ryuk ransomware group.

Ryuk, and the criminal conspiracy associated with it, had become a major focus for the NCA. Later, the agency, alongside the FBI, would expose several members of the cybercrime gang, linking them to another ransomware strain, Conti, as well as the Trickbot banking trojan.

Initially, the sheer volume of funds that the NCA had uncovered on the blockchain was shocking. "I genuinely thought that there's a decimal point wrong," said Will Lyne, the head of intelligence for the NCA's cybercrime unit.

The scale "became apparent pretty quickly," added the investigation's tactical lead, who spoke to Recorded Future News on the condition of anonymity. Blockchain analysis and other techniques allowed the investigators "to identify hundreds of millions, if not billions" being turned over. It was well beyond what they expected.

"We were still looking at this in the context of ransomware ransom payments. … We were originally thinking this is a financial service that's enabling the Ryuk business model," said Lyne, but the cyber team quickly realized that what was happening "was much broader than just our threat area."

It was relatively straightforward for the NCA to link this blockchain activity to two particular real-world entities; Russian businesses called Smart and TGR Group, both based in Moscow's landmark Federation Tower.

The head of the Smart network was Ekatarina Zhdanova — a business celebrity in Russia, and "not your typical organized crime group boss," as the NCA's director general of operations Rob Jones told journalists when the operation was first unveiled. The TGR Group was led by George Rossi, assisted by Elena Chirkinyan.

Left to right: Elena Chirkinyan, George Rossi and Ekatarina Zhdanova. Images: U.K. NCA

Both entities became part of the investigation, but the blockchain linked these potential billions of dollars to other organizations well outside of the ransomware world. It meant the investigation was becoming something much more than the cyber team's typical fare. "We quite quickly began to think of it conceptually as a Russian illicit finance and global money-laundering network operating across numerous jurisdictions, which changed our framing of the threat and the framing of our investigation," said Lyne.

"Even through a cursory search and open source, you can see how Zhdanova is connected to the Moscow social scene," said the NCA's tactical lead. "And through our review of other material, we were aware as well of the connection into wider money laundering ecosystems around the world."

Breakthrough

At that point, the investigation was a matter of high-level money laundering all taking place abroad. The major breakthrough came in November 2021, when a suspected criminal cash courier — a man called Fawad Saiedi — was arrested while driving southbound on the M1 motorway toward London with £250,000 in cash in his vehicle alongside a tranche of invaluable evidentiary material.

This material was key. The NCA now knew that as a single cash courier, Saiedi had laundered over £15,650,000. Moreover, there was evidence he had done so for Ekatarina Zhdanova in a sprawling cash-for-crypto scheme.

"It was a really important arrest and it demonstrated this cash-for-crypto activity in the U.K. in a way that I don't think we were totally unaware of, but it connected it in a way that I think was really interesting," said Lyne.

"Effectively following that arrest, and when we reviewed all of [Saiedi's] exhibits, we put together a suspicion that Zhdanova was also connected to this, as well as other key associates with links to the Smart group," said the

NCA's tactical lead.

Body camera footage of Fawad Saeidi's arrest. Image: U.K. NCA

By "exploring those links" between Zhdanova and her associates and cash couriers in the United Kingdom, the NCA eventually was "able to further connect those individuals into a series of other U.K.-based cash-to-crypto networks. Effectively, the investigation began from there and really began to flourish afterwards."

Saiedi's cash runs were being managed by a man called Nikita Krasnov, whom the NCA identified as one of Zhdanova's associates. Krasnov was ultimately also found to be coordinating other courier networks utilizing Russian-speakling individuals.

The investigators put this critical cash courier level — linking street-level dealers to international crime — under their spotlight. The NCA used a range of covert capabilities to track these couriers and the coordinators who directed them on behalf of Smart and TGR, as well as the cash and other stores of value being routed around the world, often through the United Arab Emirates.

"From the criminal perspective, cryptocurrency effectively turbo-charges [value exchanges] and speeds everything up from them. Obviously you can move value there across borders in seconds, very cheaply. And it gives criminals a form of value that they're happy to transact in, rather than having cash move from one jurisdiction to another," said the tactical lead.

Another NCA officer who can only be identified as the strategic operational lead told Recorded Future News that the realization came "very slowly" about how the different parts of this conspiracy were interconnected. "It was quite clear that it was cross-cutting, from the Russian angle into serious organized crime, but at that moment we knew that there would be a massive opportunity if we looked at it as a cross-threat thing rather than a cyber thing."

The investigation was now definitely beyond the cyber team's threat area.

Curveballs

And then the NCA encountered something it was not only not expecting, but wasn't able to investigate. Among the laundering services' clients were Russian elites using the networks to purchase property in the West, and also to RT (formerly Russia Today) — owned by an entity sanctioned by the U.K. — which used the network to fund another media organization in Britain. But while these could fall within the NCA's remit, the agency said that "from late 2022 to summer 2023 the Smart network was used to fund Russian espionage operations." Unlike in the U.S., where the FBI has a counterintelligence function as well as its work tackling serious crime, the NCA doesn't investigate state-sponsored threats such as espionage, which instead largely fall to the Security Service (MI5).

The British state's approach is strictly compartmentalized, even when cases such as this highlight the blurred distinctions between state-sponsored threats and organized crime. But for the NCA, the discovery of a state-sponsored link means handing off certain aspects of the investigation to those other parts of government, and continuing to progress its investigation into the criminal networks.

It is not known what espionage operations were funded using the Smart network. In November, two Bulgarian nationals pleaded guilty to being part of a spy ring run by a Russian agent in Britain. Three of their alleged accomplices have denied the allegations. That alleged spy ring was operational between August 2020, and February 2023 according to prosecutors, and the trial is ongoing.

As the investigation continued, the NCA interdicted 24 different cash swaps and learned of many more, often almost immediately accompanied by a transfer. One network alone was identified conducting "cash handovers in 55 different locations across England, Scotland and Wales and the Channel Islands, over a four-month period. They did so on behalf of at least 22 suspected criminal groups," according to Lyne.

Cash seized by the NCA in Operation Destabilise.

"We had multiple cash seizures in quite quick succession, which was obviously fantastic. These interdictions almost always happen over the weekend. Drug dealers seemingly don't like keeping loads of money in stash houses over the weekend," said Lyne.

“Whether it’s rival crime groups or more probably law enforcement, [they are] quite keen to get rid of the cash as soon as possible,” the tactical lead explained. “It’s a reassurance policy, ‘I’ve got rid of this big lump of cash that could easily be seized by law enforcement or whoever else it might be, rival groups. And in fact I’ve got a receipt here that proves that I’m getting back £100,000 from the money-laundering group.’ It gets rid of heavy assets that they could easily lose to something that’s slightly insured to an extent.”

Repeatedly, the the money-handling members of the drug dealing gangs were seen handing cash to the couriers in exchange for cryptocurrency — usually the dollar-linked USD Tether crypto asset — which Lyne said the NCA saw being transferred almost immediately after the handover, and believes eventually made its way to South American drug cartels to fund more shipments of cocaine.

All of these incidents provided valuable intelligence and numerous leads, both of the onward movement of cash as well as of the crypto assets. The most challenging task for the NCA was not just analyzing that intelligence effectively, but establishing a structure for the investigation with each of its many parts — from the Russia-based entities through to the coordinators and cash courier networks — all being complex investigations in and of themselves.

“We broadened it out, we had to bring in and leverage expertise from across the agency and elsewhere to make sure that we’ve got the right skill sets, and then we had to set up our governance structure to bring all of those skills cohesively together,” said Lyne.

“We recognized this was too big to be one single investigation, and so we took the decision that we would have Operation Destabilise as an almost overarching governance structure, with some leadership and decision-making, objective-setting skills,” he added.

Breaking down the investigation meant identifying distinct networks. “That’s fairly easy, if you’ve got a group of people that are co-conspiring to commit whatever offending, you clearly want to do that [investigation] as a collective,” said the strategic operational lead.

> "It’s probably the first time in 34 years I’ve seen such a variance of interconnection.”
>
> *— The strategic operational lead for the U.K. NCA's Operation Destabilise.*

Then “within that group you’ll identify the hierarchy, from there the hierarchy leads to another set of controllers, [there will be another] hierarchy there that you’ll separate off. So [you] allow [another] team to focus on that, and we’re literally breaking them [the criminal networks] up, understanding [the intelligence] within the U.K., and [then] allocating investigation teams wherever the most appropriate place is,” explained the strategic operational lead.

The NCA followed street cash being consolidated and counted and then washed through traditional high-cash turnover businesses in the United Kingdom, or simply being driven out of the country into other jurisdictions. The NCA’s Jones explained that there was simply so much money being made that no single laundering route was used and that millions of pounds are regularly smuggled across the border, despite these transfers regularly being caught.

“So the evidence you gleaned from ‘Brian Smith’ with 30,000 quid in a carrier bag can be directly linked to movements that Zhdanova’s facilitating through the international controller networks, who act as the connectors and are often located in the Middle East, and from Russia,” said the strategic operational lead. While those value movements often involved cryptocurrency, the laundering services were also seen trading property and other stores of value including shares and bonds to enrich their clients.

“It’s probably the first time that in my time we’ve seen the interconnection between global impacts and money laundering at the highest possible level, and its interconnection to street level organized crime, traditional organized crime, whether it be guns, drugs, whatever, and evolving in a new methodology of money exchanges, which is clearly changing. It’s probably the first time in 34 years I’ve seen such a variance of interconnection,” they added.

Seeing how this value was transferred internationally, particularly through the lens of the movement of crypto assets — on top of all of the other evidence that the agency was acquiring — provided the NCA with “a really good opportunity to understand the methodology as well as the connection” between both ends of the criminal world.

“When we talk about the pool data, it’s absolutely everything, you know, from handwritten notes through to digital forensics, in some cases wet forensics as well, it all gets pooled and analyzed together,” explained the tactical lead, using a term for physical forensic evidence. “The way that we pooled data from all of the different investigations under Destabilise to one place so that we had a single version of the truth for us, and the ability to analyze that material from a centralized perspective, was really powerful for us.

“And then when you combine that with blockchain activity, and especially when we can deanonymize some of that through the powers that the NCA has under the Crime and Courts Act and others, it provides a really powerful pool of data where we can effectively link this back to senior individuals and really trace it from the courier level right up to the senior Russian level,” they added.

“In terms of the complexity and the global reach, I think the scale of this is beyond anything that I’ve been involved in,” said the strategic operational lead.

The networks being investigated were “operating on local-to-global levels, and our response to it has mirrored that, tackling the street-level drug deals in towns and cities up and down the U.K., to the South American cartels and senior coordinators, all the way through to enabling Russian espionage. This is the kind of investigation the NCA was built for, in my view, and I think we’ve risen to the challenge of tackling something like this in a really holistic way,” said Lyne.

[Alexander Martin]

is the UK Editor for Recorded Future News. He was previously a technology reporter for Sky News and a fellow at the European Cyber Conflict Research Initiative, now Virtual Routes. He can be reached securely using Signal on: AlexanderMartin.79
