Notes Pro forma

Pronounced in the council chamber of the Den Bosch court. Case: Kidwelly
Parquet number : 82/198261-22
Suspect : A.O.Pertsev
Date: November 22, 2022 Public Prosecutor M. Boerlage

Dear Court, Dear Attendees,

Today is the first public hearing in the Kidwelly case. The Kidwelly case is about Tornado Cash. A cryptocurrency mixer on the Ethereum blockchain. When reading the pro forma file it was undoubtedly noticed that part of the research has a highly technical content. But appearances are deceiving. Because if you peel everything off, we are dealing here with a fairly clear money laundering case.

After all, it is prohibited (Article 420bis paragraph 1), among other things, to hide/disguise the origin and relocation of objects and to hide/disguise who is the rightful claimant to an object or to hide/disguise who owns the object. That is exactly what a mixing service like Tornado Cash does: it obscures the origin and destination of cryptocurrencies by creating a so-called “clip” between the currency that is placed in the mixer and the currency that leaves the mixer. It thus creates anonymity for the owner of crypto currency (hereinafter crypto).

And that constitutes a criminal offense if the person offering this service to the public knew, or should reasonably have suspected, that this crypto came wholly or partly, directly or indirectly, from any crime.

It is not for nothing that the use of a mixer when selling crypto has been designated by the FIU as a typology for money laundering. That also applies to the supplier of that mixer: he is forewarned.

It is suspected that Pertsev, together with a number of people, is the provider of the mixing service Tornado Cash, while he knew that criminal cryptos were laundered on a large scale via Tornado Cash. It concerns the laundering of criminal cryptos with a combined value of at least USD 1.055 billion. Analysis also seems to show that almost 75% of all cryptos originating from crime are placed on the Etherium blockchain with Tornado Cash. So Tornado Cash is the go-to mixer after a hack has taken place. That is also known to the suspect.

Role of Pertsev at Tornado Cash

It emerges from the case file that Defendant founded Peppersec INC together with S. and S. and probably developed Tornado Cash largely with that company. Tornado Cash is even their 'Magnum Opus'. That Peppersec, Tornado Cash and the suspect are closely connected is also apparent from other findings. The account details from the suspect's phone, and especially from one of the main chat groups in the Telegram app found on the suspect's phone: the chat called Bablo Peppersec (which appropriately means 'Peppersec Money'). In it, Pertsev, S. and S. have

been consulting since October 2019 and actually discuss the most important decisions that relate to the day-to-day ins and outs of Tornado Cash, the decision-making around Tornado Cash and its further development.

In AMB-19 and AMB-22, Pertsev's involvement and suspicion with Tornado Cash are further described and substantiated. The fact that he once came up with a smart contract, published the code and had nothing else to do with Tornado Cash can be relegated to the realm of fantasy in view of these findings. The suspect has been part of 'Team Tornado Cash' and has been developing Tornado Cash ever since, together with S. and S. The three of them set out the lines. Not only will a decentralized mixing protocol come online, but a User Interface will also be developed, a relay system will be installed, a Dune dashboard, etc. The Defendant was working on this up to the day of his arrest.

This is important because it shows that the Defendant had an influence on the operation of Tornado Cash, he helped determine whether and if so how customers could access the mixing protocol (the User Interface) and how customers could receive cryptos again via the relayer system.

Outwardly, the protocol may have been pretended to be "governed" by the Community (a so-called DAO). In practice, Pertsev, S. and S. had great influence by directing the content of the proposals. The investigation also shows that the Defendant and his companions influenced the decision-making process: not only did they vote together in a number of cases (this is currently being investigated), but they also influence the positions of those they did or didn’t want to vote. And apparently they decide when the vote takes place.

In combination with the fact that they own by far the most TORN tokens (which are needed to vote), the suspect, S. and S., can always outvote everyone. That means they actually have control about what was or wasn't going to happen within the community of Tornado Cash.

In addition, the three men assign various tasks to others, to employees, and Pertsev also gets angry when work is poor. In the Bablo Peppersec chat it is explicitly discussed that – after the OFAC sanctions – the team does not have to worry about salary, that everything is fine with the money. Apparently there are people on the payroll and the suspect and S. and S. are responsible.

The three men are also thinking about external communication. For example, it is discussed (and also implemented) that there should be a standard response to outsiders who ask for help (namely that they unfortunately cannot do anything). But other messages are also submitted to them and not published before they have given permission. Finally, like any board of a company, they have contact with lawyers and accountants about business matters.

In short, the Defendant, together with S. and S., is in the 'driver's seat' and therefore actually determines what does or does not happen within Tornado Cash.

Pertsev's knowledge
Pertsev was one of the main developers of Tornado Cash, so he knew in detail about the functioning of the entire Tornado Cash ecosystem and therefore also about the shortcomings. For some time now, there has been a great deal of attention in the media for hacks and mixing services that are used to keep the loot out of sight of the rightful claimants and the investigative services. Tornado Cash was also explicitly referred to in the press.

Several requests from both law enforcement and the private sector were found on Pertsev's phone indicating that Tornado Cash was being used to deliver and keep stolen crypto from its rightful owners with a request for help.

Finally, there is also discussion among themselves, with S. and S., about the fact that criminals use Tornado Cash. The solution they propose: attract more crypto from non-criminals. And therefore not: keep criminal crypto out. They also decide to refrain from a publication on Twitter describing various ways to circumvent AML. Better not, they discuss, then it could be pointed out that they offer 'shady stuff'. They just decide not to, especially now after 2 hacks for 100+. In other words, they support the message, but realize that it does not look good to the outside world to give anti-AML advice. Other hacks are also shared among themselves.

The most notable is the Ronin Bridge hack. As early as March 29, 2022, this link will be shared in Bablo Peppersec, including the amount of $600 million in stolen crypto. CoinDesk also reached out to the suspect that day, asking how such an amount could be laundered. Not surprising, given the many publications that show that Tornado Cash has also been used in other hacks to get rid of the loot. We now know that from March 4 (so well after the suspect became aware) until May 19, 2022, cryptos originating from this hack were placed in Tornado Cash on various days and that on those days an average of 51% (with a peak of 79%) of all postings came from this hack. Mind you, these are huge sums, all of which were only placed in the main pool of 100ETH. This is comparable to someone who only deposits large stacks of €100 notes at the bank. If you as a bank do not know who it is, do not know where the money comes from and have not built in any mechanism to look at it, then you accept the considerable chance that you are laundering money with your service to the public.

Possibilities for intervention by Pertsev
The research team then investigated whether there were options for Pertsev to prevent large-scale laundering through Tornado Cash. That investigation showed that the only recently implemented compliance tool (so it was possible!), to exclude certain sanctioned addresses (oracle), was substandard. And that there were indeed other possibilities to build in controls with regard to the origin of the cryptos. So there were, in fact: for Pertsev, S. and S. in April 2022 it is apparently just a 'brainS. idea', which is therefore deliberately not chosen.

Statement of Pertsev
To date, Pertsev has offered little or nothing as explanation. He has indicated since August that he wants to make a statement, but to do so in his own way by means of a written statement. To

date, that written statement has not been issued and it is unknown when it will come. For now this means that:
- If substantiated research results are not contradicted, the Public Prosecution Service assumes that they are correct
- The investigation takes longer (for example, because the laptop still needs to be unlocked)

Conclusion
The Defendant therefore knew that cryptos originating from crime (including theft, hacks) were being passed through Tornado Cash on a large scale, not only had the knowledge, but also the influence to do something about it.

He deliberately chose to allow the situation to exist, that more than 1 billion in criminal cryptos were passed through his mixer. In that circumstance, you are knowingly accepting the significant likelihood that the service you are offering to the public is a large-scale money laundering activity. That you are knowingly hiding and conceal what the actual origin of the cryptos is, how and where they were moved and who the actual rightful holder is.

Pertsev also had no reason to intervene: after all, he earned a good living from Tornado Cash. As mentioned earlier, he received wages from Peppersec, in addition to receiving a large amount of TORN tokens. Which of course, the more successful Tornado Cash was, got a higher value. In other words: the Defendant also had every interest in keeping the volume of Tornado Cash as large as possible. Not really an incentive to do transaction monitoring, that not only costs money and effort, but you will probably also lose a large part of your customers. After all: the anonymity that Tornado Cash brings is the biggest selling point. Not for nothing that hackers loved to visit Tornado Cash.

It is suspected that the Defendant also earned money from Tornado Cash in other ways, but this is still being investigated. However, large amounts of cryptos in the name of the suspect have been found in various places in the world. He also has several bank accounts abroad that are being investigated further. The fact that the suspect and his wife only live on his wages from Peppersec is in any case out of the question, as he would not be able to pay for his rented house and expensive Porsche from that.

Pre-trial detention.
<u>Seriousness of the facts:</u>
The suspect has, it is suspected, been involved in the professional laundering of at least 1 billion dollars in crypto. This for a longer period of time, knowingly co-organized and maintained. This crypto all comes from crime, from theft, from hacks. So there are - all over the world - victims who have lost this crypto and - also all over the world - perpetrators of these hacks who are permanently enriched with this crypto because the suspect has laundered them for them. By offering this criminal service, the Defendant has also ensured that cryptocurrency services get a bad name. The general public is getting the feeling that they cannot safely dispose of cryptos.

Defendant has also not given any openness about the matter, hardly answers questions. That is of course his right, but that also means that the investigation takes longer. For example, there is still no access to his laptop, while these facts were actually committed with this laptop. Important evidence has not yet been unlocked and can still potentially be erased if released.

Flight Hazard:
The suspect has Russian nationality. If he is released and returns to Russia, he will avoid justice. After all, Russia does not extradite its citizens. It is a naive idea that he stays here because of work, while a considerable prison sentence hangs over his head. In addition, the suspect has an employment contract with Expatrix. Expatrix was hired by Peppersec. And since the Defendant, together with S. and S. is Peppersec, the Defendant actually had himself hired by his own company via a detour. Expatrix has canceled the contract and also reported this to the IND. This means that the grounds for residence in the Netherlands have lapsed. I also note that the Defendant – at the time of his arrest – was busy arranging flights abroad. It was suspected that he wanted to leave for Turkey.

Risk of Collusion:
There is a danger that if the suspect is released, digital evidence will be lost. That this is a real danger is apparent from the fact that after the arrest of the suspect, an attempt was made to conceal the involvement of the suspect (and S. and S.). We are still awaiting various research results from abroad, especially with regard to relayers and money/cryptocurrencies abroad. Such an investigation, especially now that the suspect does not want to answer any questions about it, simply takes a long time. Such evidence and such money and crypto flows are digitally accessible from anywhere in the world if you know where to look and how to access them. The suspect knows this better than anyone. He has every interest in further concealing and/or deleting this information from investigative services.

Risk of recidivism:
The fact that the information report announces that the suspect will return to work at Peppersec upon release means that the Public Prosecution Service has no confidence whatsoever in the promise that the suspect will no longer work on software comparable to Tornado Cash. Peppersec IS Tornado Cash. The offenses that the suspect is suspected of are committed online, the only thing that the suspect needs is the internet and a computer. Work, ET and contact with the probation service do not remove the danger of collusion and recidivism. And flight risk is not reduced by this either.

This means that the Public Prosecution Service sees no reason to suspend. The report submitted by counsel does not change that. With such serious facts and grounds present, a compelling personal interest will have to be put forward. Nothing has turned up. In addition, the stated conditions do not remove the grounds.