Aantekeningen
Pro forma

OPENBAAR MINISTERIE

Functioneel Parket, HHE Zwolle

Uitgesproken in de raadkamer van de rechtbank Den Bosch

Zaak	:	Kidwelly
Parketnummer	:	82/198261-22
Verdachte	:	A.O.Pertsev
Datum	:	22 november 2022

Officier van justitie mr. M. Boerlage

Geachte rechtbank, geachte aanwezigen,

Vandaag is de eerste openbare zitting in de zaak Kidwelly. In de zaak Kidwelly gaat over Tornado Cash. Een cryptovaluta mixer op de Etherium blockchain. Bij het lezen van het pro forma dossier is ongetwijfeld opgevallen dat een deel van het onderzoek een hoog technisch gehalte heeft. Maar de schijn bedriegt. Want als je alles afpelt hebben we hier te maken met een vrij overzichtelijke witwaszaak.

Immers het is (artikel 420bis lid 1 onder a Sr) onder meer verboden om van voorwerpen de herkomst en verplaatsing te verbergen/verhullen en te verbergen/verhullen wie de rechthebbende op een voorwerp is of te verbergen/verhullen wie het voorwerp voorhanden heeft. Dat is precies wat een mixing service zoals Tornado Cash doet: het verhult de herkomst en de bestemming van cryptovaluta door een zogenaamde 'knip' te zetten tussen de valuta die in de mixer wordt geplaatst en de valuta die de mixer weer verlaat. Het creëert daarmee anonimiteit voor de bezitter van cryptovaluta (hierna crypto's).

En dat levert een strafbaar feit op als degene die deze dienst aan het publiek aanbiedt wist, dan wel redelijkerwijs moest vermoeden dat deze crypto's geheel of gedeeltelijk, onmiddellijk of middellijk afkomstig waren uit enig misdrijf.

Het is ook niet voor niets dat het gebruik van een mixer bij de verkoop van crypto's door de FIU is aangemerkt als een typologie voor witwassen. Dat geldt dus net zo goed voor de aanbieder van die mixer: die is dus een gewaarschuwd mens.

De verdenking is dat Pertsev samen met een aantal personen de aanbieder is van de mixingdienst Tornado Cash terwijl hij wist dat er via Tornado Cash op grote schaal uit misdrijf afkomstige crypto's werden witgewassen. Het gaat om het witwassen van criminele crypto's met een gezamenlijke waarde van tenminste 1.055 miljard dollar. Uit analyse lijkt ook naar voren te komen dat bijna 75% van alle uit misdrijf afkomstige crypto's op de Etherium blockchain bij Tornado Cash worden geplaatst. Tornado Cash is dus de 'go-to' mixer nadat er een hack heeft plaatsgevonden. Dat is ook bij verdachte bekend.

<u>Rol Pertsev bij Tornado Cash</u>
Uit het dossier komt naar voren dat verdachte, samen met S. en S. Peppersec INC hebben opgericht en vermoedelijk grotendeels met dat bedrijf Tornado Cash hebben ontwikkeld. Tornado Cahs is zelfs hun 'Magnum Opus'. Dat Peppersec, Tornado Cash en verdachte nauw met elkaar verbonden zijn blijkt ook uit andere bevindingen. De accountgegevens van telefoon van verdachte, en vooral uit een van de belangrijkste chatgroep in de app Telegram die op te telefoon van verdachte is aangetroffen: de chat genaamd Bablo Peppersec (wat heel toepasselijk 'Poen Peppersec betekent). Hierin overleggen Pertsev, S. en S. sinds oktober 2019 en bespreken feitelijk de belangrijkste beslissingen die betrekking hebben op het dagelijkse reilen en zeilen van Tornado Cash, de besluitvorming rond Tornado Cash en de verdere ontwikkeling.

In AMB-19 en AMB-22 zijn de betrokkenheid en verdenking van Pertsev bij Tornado Cash nader beschreven en onderbouwd. Dat hij ooit een keer een smart contract heeft bedacht, de code gepubliceerd heeft en verder niets meer met Tornado Cash te maken heeft gehad, kan gelet op deze bevindingen naar het rijk der fabelen worden verwezen. Verdachte maakt sinds 2019 onderdeel uit van

‘Team Tornado Cash’ en is sindsdien, samen met S. en S., bezig met het ontwikkelen van Tornado Cash. Zij zetten gedrieën de lijnen uit. Niet alleen komt een gedecentraliseerd mixingprotocol online maar er wordt ook een User Interface ontwikkeld, er komt een relayer-systeem, een Dune-dashboard etc. Verdachte was hier tot op de dag van zijn arrestatie mee bezig.

Dat is van belang omdat dit laat zien dat verdachte invloed had op de werking van Tornado Cash, hij bepaalde mede of en zo ja hoe klanten het mixingprotocol konden benaderen (de User Interface) en op welke wijze klanten via het relayer-systeem crypto’s weer konden opnemen.
Naar buiten toe werd misschien gedaan alsof het protocol ‘bestuurd werd’ door de Community (een zogenaamde DAO). In de praktijk hadden Pertsev, S. en S. grote invloed door te sturen op de inhoud van de proposals. Ook blijkt uit het onderzoek dat verdachte en zijn companen invloed hadden op de besluitvorming: niet alleen stemden ze in een aantal gevallen mee (daar wordt op dit moment nog onderzoek naar gedaan), maar sturen ook op personen die zij wel of juist niet op posities willen hebben waar gestemd wordt. En blijkbaar bepalen zij wanneer de stemming plaatsvindt.

In combinatie met het feit dat zij verreweg de meeste TORN-tokens bezitten (die nodig zijn om mee te stemmen) kunnen verdachte, S. en S., altijd iedereen overstemmen. Dat maakt dat zij feitelijk zeggenschap hadden over wat er wel of niet ging gebeuren binnen de ‘community’ Tornado Cash.

Daarnaast worden door het driemanschap diverse taken uitgezet bij anderen, bij werknemers, en wordt Pertsev ook boos als er slecht werk wordt geleverd. In de chat Bablo Peppersec wordt uitdrukkelijk besproken dat — na de OFAC-sancties — het team zich geen zorgen hoeft te maken over het salaris, dat alles in orde is met het geld. Blijkbaar staan er mensen op de loonlijst en is verdachte met S. en S. verantwoordelijk.
Ook over de externe communicatie wordt door het driemanschap nagedacht. Zo wordt besproken (en ook uitgevoerd) dat er een standaard reactie moet komen richting buitenstaanders die om hulp vragen (namelijk dat zij helaas niets kunnen doen). Maar ook andere berichten worden aan hun voorgelegd en niet gepubliceerd voordat zij toestemming hebben gegeven. Tot slot hebben zij — zoals elk bestuur van een bedrijf — contact met advocaten en boekhouders over bedrijfsmatige kwesties.

Kortom, verdachte zit, samen met S. en S. in de ‘drivers seat’ en bepaalt dus feitelijk wat er wel of niet binnen Tornado Cash gebeurt.

<u>Wetenschap Pertsev</u>
Pertsev was één van de belangrijkste ontwikkelaar van Tornado Cash, hij was dus tot in detail op de hoogte van de werking van het gehele ecosysteem Tornado Cash en daarmee ook van de tekortkomingen. In de media was al langere tijd grote aandacht voor hacks en mixerdiensten die gebruikt worden om de buit uit het zicht van de rechthebbenden en de opsporingsdiensten te houden. In de pers werd ook telkenmale uitdrukkelijk naar Tornado Cash verwezen.
Op de telefoon van Pertsev zijn diverse verzoeken aangetroffen van zowel politiediensten als de private sector waarin werd aangegeven dat Tornado Cash werd gebruikt om gestolen crypto uit handen te brengen en houden van de rechtmatige eigenaren. Met een verzoek om hulp.

Tot slot wordt ook onderling, met S. en S. gesproken over het feit dat criminelen gebruik maken van Tornado Cash. De oplossing die ze aandragen: meer crypto’s

van niet criminelen aantrekken. En dus niet: criminele crypto's weren. Ook besluiten ze af te zien van een publicatie op twitter waarin diverse manieren worden beschreven om AML te omzeilen. Beter van niet, zo bespreken ze, dan zou er naar ze gewezen kunnen worden, dat ze 'shady stuff' aanbieden. Ze beslissen het maar niet te doen, *vooral nu na 2 hacks voor 100+*. Met andere woorden: ze staan wel achter de boodschap, maar zien in dat het er richting de buitenwereld niet goed uitziet om anti-AML advies te geven. Ook andere hacks worden onderling gedeeld.
De meest opvallende is de Ronin Bridge hack. Al op 29 maart 2022 wordt deze link in Bablo Peppersec gedeeld, inclusief het bedrag van 600 miljoen dollar aan gestolen crypto. Coindesk komt die dag ook bij verdachte op de lijn, met de vraag hoe een dergelijk bedrag kan worden witgewassen. Niet vreemd, gelet op de vele publicaties waaruit blijkt dat Tornado Cash ook bij andere hacks is gebruikt om de buit weg te maken. Inmiddels weten we dat vanaf 4 maart (dus ruim nadat verdachte op de hoogte raakte) tot en met 19 mei 2022 op diverse dagen crypto's afkomstig van deze hack in Tornado Cash zijn geplaatst en dat op die dagen gemiddeld 51% (met een uitschieter naar 79%) van alle plaatsingen afkomstig waren van deze hack. Let wel: het gaat hier om enorme bedragen, die allemaal enkel in de grote pool van 100ETH werden geplaatst. Dit is vergelijkbaar met iemand die alleen maar met grote stapels briefjes van € 100 bij de bank komt storten. Als je als bank niet weet wie het is, niet weet waar het geld vandaan komt en ook geen enkel mechanisme hebt ingebouwd om daar naar te kijken, dan aanvaard je de aanmerkelijke kans dat je met jouw dienst aan het publiek aan het witwassen bent.

<u>Mogelijkheden tot ingrijpen door Pertsev</u>
Door het onderzoeksteam is vervolgens nog onderzocht of er voor Pertsev mogelijkheden waren om te voorkomen dat er op grote schaal werd witgewassen via Tornado Cash. Uit dat onderzoek bleek dat de enige, recent geïmplementeerde compliance-tool (het kon dus wel!), om bepaalde gesanctioneerde adressen te weren (oracle), ondermaats was. En dat er wel degelijk andere mogelijkheden waren om controles in te bouwen met betrekking tot de herkomst van de crypto's. Die waren er dus wel, sterker nog: het is voor Pertsev, S. en S. in april 2022 blijkbaar slechts een 'brainS. idee', waar dus bewust niet voor gekozen wordt.

<u>Verklaring Pertsev</u>
Tot op heden heeft Pertsev weinig tot niets willen verklaren. Hij geeft al sinds augustus aan dat hij een verklaring wil afleggen, maar dit op zijn manier doet middels een schriftelijke verklaring. Tot op heden is die schriftelijke verklaring er niet en is onbekend wanneer deze zal komen. Vooralsnog betekent dit dat:

- Als onderbouwde onderzoeksresultaten niet worden tegengesproken het Openbaar Ministerie er vanuit gaat dat deze kloppen
- Het onderzoek langer duurt (bijvoorbeeld omdat de laptop nog steeds moet worden ontsloten)

<u>Conclusie</u>
Verdachte wist dus dat er op grote schaal van misdrijf (o.a. diefstal, hacks) afkomstige crypto's door Tornado Cash gingen, had niet alleen de kennis, maar ook de invloed om daar iets aan te doen. Hij koos er bewust voor om de situatie te laten bestaan, dat ruim 1 miljard aan criminele crypto's door zijn mixer werden gehaald. Onder die omstandigheid aanvaard je willens en wetens de aanmerkelijke kans dat je met de dienst die je aan het publiek aanbiedt op grote schaal aan het witwassen bent. Dat je willens en wetens aan het verbergen en

verhullen bent wat de daadwerkelijke herkomst van de crypto's is, hoe en waarheen die verplaatst zijn en wie de daadwerkelijke rechthebbende is.
Pertsev had ook geen enkele reden om in te grijpen: immers hij verdiende een goede boterham aan Tornado Cash. Zoals eerder aangegeven, hij ontving loon van Peppersec, en daarnaast kreeg hij de beschikking over een grote hoeveelheid TORN-tokens. Die uiteraard, hoe succesvoller Tornado Cash was, een hogere waarde kregen. Met andere woorden: verdachte had er ook alle belang bij om het volume van Tornado Cash zo groot mogelijk te houden. Niet echt een incentive om aan transactiemonitoring te gaan doen, dat kost niet alleen geld en moeite, maar je verliest vermoedelijk ook een groot deel van je klanten. Immers: de anonimiteit die Tornado Cash brengt is het grootste 'selling point'. Niet voor niets dat hackers graag bij Tornado Cash langskwamen.

Het vermoeden is dat verdachte ook nog op andere manieren aan Tornado Cash verdiende, maar daar wordt nog nader onderzoek naar gedaan. Wel zijn er op diverse plekken in de wereld grote bedragen aan crypto's op naam van verdachte aangetroffen. Ook heeft hij diverse bankrekeningen in het buitenland waar nader onderzoek naar wordt gedaan. Dat verdachte en zijn vrouw enkel leven van zijn loon uit Peppersec is in ieder geval uitgesloten, daar zou hij zijn huurhuis en dure Porsche niet van kunnen betalen.

<u>Voorduren voorlopige hechtenis.</u>

Ernst van de feiten:
Verdachte heeft zich, zo is de verdenking, bezig gehouden met het professioneel witwassen van tenminste 1 miljard dollar aan crypto's. Dit gedurende langere tijd, willens en wetens mede georganiseerd en in stand gehouden. Deze crypto's zijn allen afkomstig van misdrijf, van diefstal, van hacks. Er zijn dus — over de hele wereld — slachtoffers die deze crypto's kwijt zijn en — tevens over de hele wereld — daders van deze hacks die blijvend verrijkt zijn met deze crypto's omdat verdachte deze voor hen heeft witgewassen. Door deze criminele dienst aan te bieden heeft verdachte er tevens voor gezorgd dat cryptovaluta-diensten een slechte naam krijgen. Het grote publiek krijgt het gevoel dat zij niet veilig over crypto's kunnen beschikken.

Verdachte heeft ook geen openheid van zake gegeven, geeft nauwelijks antwoord op vragen. Dat is uiteraard zijn recht, maar dat betekent ook dat het onderzoek langer duurt. Zo is er nog geen toegang tot zijn laptop, terwijl deze feiten feitelijk met deze laptop zijn gepleegd. Belangrijk bewijs is daarmee nog niet ontsloten en kan in potentie nog steeds worden gewist als hij vrij komt.

Vluchtgevaar:
Verdachte heeft de Russische nationaliteit. Als hij wordt vrijgelaten en naar Rusland terugkeert ontloopt hij zijn berechting. Immers Rusland levert geen onderdanen uit. Dat hij hier blijft in verband met werk, terwijl er een aanzienlijke gevangenisstraf boven zijn hoofd hangt is een naïeve gedachte. Daarbij komt dat verdachte een arbeidscontract bij Expatrix heeft. Expatrix was ingehuurd door Peppersec. En aangezien verdachte, samen met S. en S. Peppersec is, heeft verdachte zich dus feitelijk via een omweg door zijn eigen bedrijf laten inhuren. Expatrix heeft het contract opgezegd en dit ook aan de IND gemeld. Daarmee is de grond voor verblijf in Nederland komen te vervallen. Ook merk ik op dat verdachte — ten tijde van zijn arrestatie — bezig was vluchten naar het buitenland te regelen. Het vermoeden was dat hij naar Turkije wilde vertrekken.

Collusiegevaar:

Het gevaar bestaat dat als verdachte wordt vrijgelaten er digitaal bewijs wordt weggemaakt. Dat dit een reëel gevaar is blijkt uit het feit dat na de aanhouding van verdachte ook daadwerkelijk getracht is betrokkenheid van verdachte (en S. en S.) te verhullen. Wij zijn nog steeds in afwachting van diverse onderzoeksresultaten uit het buitenland, met name ook met betrekking tot relayers en geld/cryptostromen in het buitenland. Dergelijk onderzoek, zeker nu verdachte daar geen vragen over wil beantwoorden, duurt nou eenmaal lang. Dergelijk bewijs en dergelijke geld- en cryptostromen zijn op elke plek ter wereld digitaal toegankelijk als je weet waar je moet zoeken en hoe je toegang krijgt. Verdachte weet dat als geen ander. Hij heeft er alle belang bij om deze informatie voor opsporingsdiensten verder te verbergen en/of te wissen.

Recidivegevaar:
Dat in het voorlichtingsrapport wordt aangekondigd dat verdachte bij vrijlating weer aan het werk gaat bij Peppersec maakt dat het Openbaar Ministerie geen enkel vertrouwen heeft in de belofte dat verdachte niet meer gaat werken aan software die vergelijkbaar is met Tornado Cash. Peppersec IS Tornado Cash. De feiten waar verdachte van verdacht wordt, worden online gepleegd, het enige dat verdachte nodig heeft is internet en een computer. Werk, ET en contact met de reclassering nemen het gevaar van collusie en recidive niet weg. En ook vluchtgevaar wordt hier niet door verminderd.

Dat betekent dat het Openbaar Ministerie geen enkele reden ziet om tot schorsing over te gaan. Het door de raadsman ingediende rapport brengt daar geen verandering in. Bij dergelijke ernstige feiten en aanwezige gronden zal een zwaarwegend persoonlijk belang moeten worden aangevoerd. Daar is niets van gebleken. Daarnaast nemen de aangegeven voorwaarden de gronden niet weg.