Tornado.cash sanctions

Context

Tornado Cash is a decentralized crypto mixer, which serves to hide blockchain transaction trails – making it difficult for investigators to follow the money from criminal activity. Officially, Tornado advertised itself as an anonymity tool for those seeking to enhance their financial privacy. However, this functionality made it highly attractive to cybercriminals and state-backed hacking groups – including some of the world's most notorious cyberhackers.

Last August, the US Treasury Department issued sanctions to Tornado.cash, banning Americans from using the service and spreading fear in an already fragilized ecosystem. Indeed, according to the aforementioned authority, the popular cryptocurrency mixing platform has allegedly helped launder over $7 billion worth of virtual currency since 2019[1]. These sanctions are similar to those imposed in May 2022 to Blender.io, another cryptocurrency mixing service. Several days after this episode, the Dutch Fiscal Information and Investigation Service arrested Alexey Pertsev, Tornado.cash's presumed founder.

Ambiguous justifications

It remains unclear whether it is the service itself or its usage that led the Treasury Department to ratify this harsh decision. While blockchain analytics firm Elliptic testified at least $1.5 billion in proceeds from crimes such as ransomware, hacks and fraud have been laundered through Tornado.cash[2], the American authority claimed it rose to $7 billion. This amount is obviously a bold assumption since it is literally the total value of crypto assets that flowed through Tornado's smart contracts. Besides, maintaining or contributing to the project's GitHub now exposes American developers to legal sanctions, as it is now illegal for US-based Ethereum nodes to validate incoming and outgoing transactions linked to Tornado's contracts.

Ethereum's cofounder Vitalik Buterin reacted publically the day after the Office of Foreign Assets Control (OFAC), a watchdog of Treasury's, added Tornado.cash and its 38 associated Ethereum-based addresses to its Specially Designated Nationals (SDN) list. Within a Twitter conversation, the infamous software engineer outed himself as someone who had used Tornado.cash for charity[3], in order to protect the receivers' privacy rather than

---

[1] https://home.treasury.gov/news/press-releases/jy0916

[2] https://hub.elliptic.co/analysis/tornado-cash-mixer-sanctioned-after-laundering-over-1-5-billion/

[3] https://twitter.com/VitalikButerin/status/1556925602233569280?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1556925602233569280%7Ctwgr%5E25c9fadb40a951dbcb867e39ddcb8bfd43170e92%7Ctwcon%5Es1_c10&ref_url=https%3A%2F%2Fcryptoast.fr%2Fvitalik-buterin-devoile-avoir-utilise-tornado-cash-ukraine%2F

his. Jeff Coleman, the Ethereum-based startup founder who originated the latter conversation, depicted Tornado.cash as a secure and privacy-preserving way to send funds to Ukraine, notably on Russian grounds.

Developers of Tornado Cash have responded to the sanctions in a statement released through its online social media channels, emphasizing its belief that users have a “natural right to privacy”. The statement also notes that its functioning as a decentralized autonomous organization impedes on its ability to prevent bad actors from using the service. Once again, Vitalik Buterin - along with Uniswap founder and Kraken CEO - has voiced support for Tornado.cash founder Alexey Pertsev, since his only mistake was to write open-source code that has been diverted afterwards by money launderers. However, an intelligence firm has revealed Alexey has worked for Digital Security OOO, a US-sanctioned Russian-based firm linked to the FSB, also known as KGB’s successor.

Furthermore, it seems that it is the obvious link with criminal organizations that led the US Treasury Department to ban Tornado.cash. Besides being the largest virtual currency heist ever recorded, it has been discovered the $620 million hack of Ronin Bridge had been exploited by the Lazarus Group, a Democratic People’s Republic of Korea state-sponsored hacking group that was sanctioned by the US in 2019. Additionnally, according to Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson, Tornado Cash has repeatedly failed to impose effective controls designed to stop it from laundering funds for malicious cyber actors on a regular basis and without basic measures to address its risks. Treasury will continue to aggressively pursue actions against mixers that launder virtual currency for criminals and those who assist them.

Alternatives to Tornado.cash

To begin with, using privacy-preserving crypto currencies such as ZCash or Monero might not be the panacea to perform anonymized transactions. Indeed, since you need to buy the latter coins beforehand, most of the transactions would require the help of centralized services. However, some centralized exchanges such as Huobi have stopped trading privacy coins to stick to the regulation[4]. Furthermore, such mixers are centralized and thus require the user’s trust.

On one hand, several decentralized mixing platforms remain in service in spite of the US sanctions. We can assume this is because their link with criminal organizations is yet to be exposed. On the other hand, the fact Elliptic *knew* (yet it remains unclear how they did) Tornado.cash had dealt with $1.5 billion fraudulent transactions shows de-anonymization attacks are possible. For example, the company claimed it was able to trace crypto stolen from Harmony to several new ether wallets. However, we don’t know whether Elliptic used on-chain data to perform these de-anonymization attacks or if they correlated external data sources, such as validators nodes sniffing to track suspicious IP addresses’ activity. Nonetheless, since on-chain mixers work the same, we cannot be sure whether they are also demixing-prone.

[4] https://coingeek.com/huobi-delists-monero-zcash-and-other-privacy-coins-amid-regulatory-pressure/

Conclusion

Making our own tumbler will not end up in legal sanctions as long as we can assess that no criminal organization has interacted with our services and that we do not facilitate heists, ransomware schemes, fraud and other cybercrimes. We can prevent this use case by deploying our application to the sole test net for academic purposes. Keeping the project closed-sourced may allow mitigate risks. As the US Treasury Department states[5], it will continue to investigate the use of mixers for illicit purposes and use its authorities to respond to illicit financing risks in the virtual currency ecosystem, not the development of platforms that could help anonymize transactions.

[5] https://home.treasury.gov/news/press-releases/jy0916