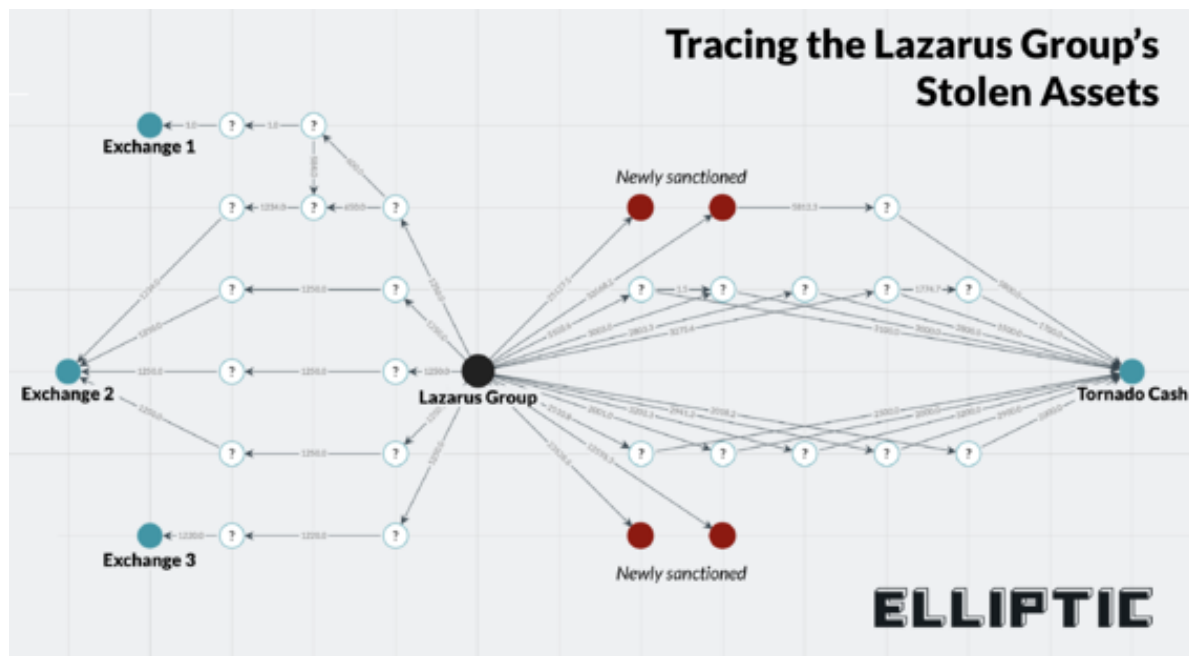
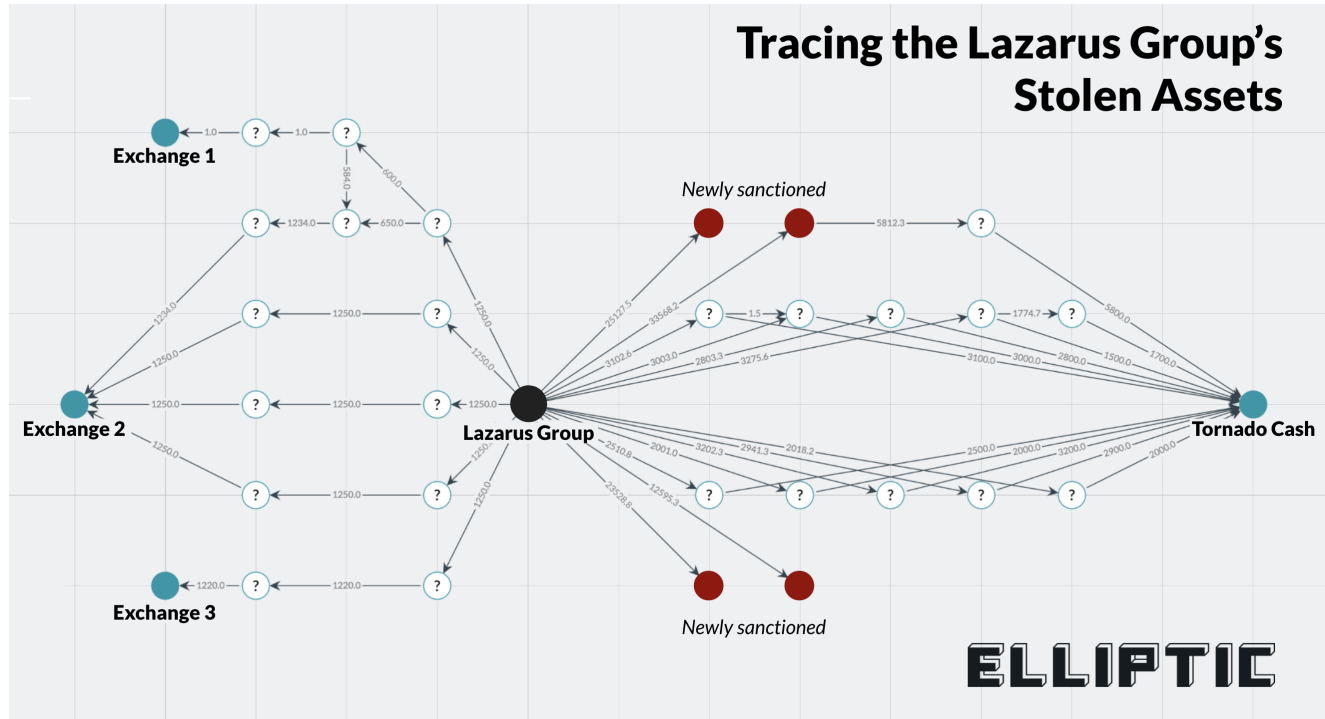


# OFAC Sanctions Virtual Asset Mixer For the First Time to Combat North Korea's Lazarus Group

 [elliptic.co/blog/ofac-sanctions-virtual-asset-mixer-for-the-first-time-to-combat-north-koreas-lazarus-group](https://elliptic.co/blog/ofac-sanctions-virtual-asset-mixer-for-the-first-time-to-combat-north-koreas-lazarus-group)



Elliptic Intel

---

**The US Treasury has initiated a fresh effort to prevent the continued laundering of the funds stolen from Ronin Bridge on March 29th by North Korea's Lazarus Group. For the first time, sanctions have also targeted the Bitcoin mixer Blender.io, which is designed to obfuscate blockchain transactions.**

The sanctions – issued by the US Office of Foreign Assets Control (OFAC) – targeted 45 Bitcoin addresses linked to Blender.io and four new wallets linked to the Lazarus Group.

## **Lazarus Group**

---

On March 29th, the North Korean cyberhacking organization stole \$540 million from a decentralized protocol allowing users to bridge their assets between Ethereum and the popular blockchain game Axie Infinity. The heist was the second largest crypto theft of all time.

As previously identified, the Lazarus Group began laundering its funds through centralized exchanges and the popular Ethereum-based mixer Tornado Cash, which announced soon after that it would be complying with US-based sanctions. It was previously believed that the Lazarus Group had moved some of the stolen funds into Bitcoin. Today's sanctioning of Blender.io appears to confirm this.

Between April 24th and May 4th, the Lazarus Group sent around \$273.9 million of Ether to the four newly-sanctioned addresses. The transactions involved amounts significantly larger than its previous laundering efforts. The ramping up of laundering efforts in this manner potentially reflects a growing desperation by the hackers, who were previously targeted with sanctions by OFAC on the 14th and 22nd of April.

One of the addresses sanctioned today had already managed to send around \$37 million through Tornado Cash prior to the sanctions announcement – leaving just over \$236 million in the sanctioned addresses.

## **Blender.io**

---

Furthermore, in a continued effort to combat money laundering by the Lazarus Group, today's actions mark the first time in which a virtual currency mixer has been sanctioned. According to an OFAC press release, Blender.io has been used by North Korea to support its money laundering activities – including the laundering of over \$20.5 million connected to the Ronin hack.

Elliptic's analysis indicates that Blender.io has also previously been used to launder funds from Hydra market, a Russian language darknet market which was sanctioned by OFAC earlier this month.

**Elliptic has taken urgent action to label the newly sanctioned addresses in our systems. Our customers will now be able to screen and be alerted for any activity relating to these addresses. View our [transaction monitoring](#) and [screening tools](#) to find out more or [contact us for a demo](#).**

**You can also download Elliptic's [Guide to Sanctions Compliance in Cryptocurrencies](#) for case studies and examples of how to use blockchain analytics for OFAC compliance.**

## **Disclaimer**

---

This blog is provided for general informational purposes only. By using the blog, you agree that the information on this blog does not constitute legal, financial or any other form of professional advice. No relationship is created with you, nor any duty of care assumed to you, when you use this blog. The blog is not a substitute for obtaining any legal, financial or any other form of professional advice from a suitably qualified and licensed advisor. The information on this blog may be changed without notice and is not guaranteed to be complete, accurate, correct or up-to-date.