

# Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over \$3 Billion of Unlawful Transactions

[justice.gov/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3](https://www.justice.gov/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3)



Press Release

Wednesday, March 15, 2023

## For Immediate Release

Office of Public Affairs

Vietnamese Operator of ChipMixer Charged with Laundering Money for Ransomware Perpetrators, Darknet Markets, Fraudsters, and State-Sponsored

The Justice Department announced today a coordinated international takedown of ChipMixer, a darknet cryptocurrency “mixing” service responsible for laundering more than \$3 billion worth of cryptocurrency, between 2017 and the present, in furtherance of, among other activities, ransomware, darknet market, fraud, cryptocurrency heists and other hacking schemes. The operation involved U.S. federal law enforcement’s court-authorized seizure of two domains that directed users to the ChipMixer service and one Github account, as well as the German Federal Criminal Police’s (the Bundeskriminalamt) seizure of the ChipMixer back-end servers and more than \$46 million in cryptocurrency.

Coinciding with the ChipMixer takedown efforts, Minh Quốc Nguyễn, 49, of Hanoi, Vietnam, was charged today in Philadelphia with money laundering, operating an unlicensed money transmitting business and identity theft, connected to the operation of ChipMixer.

“This morning, working with partners at home and abroad, the Department of Justice disabled a prolific cryptocurrency mixer, which has fueled ransomware attacks, state-sponsored crypto-heists and darknet purchases across the globe,” said Deputy Attorney General Lisa Monaco. “Today’s coordinated operation

reinforces our consistent message: we will use all of our authorities to protect victims and take the fight to our adversaries. Cybercrime seeks to exploit boundaries, but the Department of Justice’s network of alliances transcends borders and enables disruption of the criminal activity that jeopardizes our global cybersecurity.”

“Today’s announcement demonstrates the FBI’s commitment to dismantling technical infrastructure that enables cyber criminals and nation-state actors to illegally launder cryptocurrency funds,” said FBI Deputy Director Paul Abbate. “We will not allow cyber criminals to hide behind keyboards nor evade the consequences of their illegal actions. Countering cybercrime requires the ultimate level of collaboration between and among all law enforcement partners. The FBI will continue to elevate those partnerships and leverage all available tools to identify, apprehend and hold accountable these bad actors and put an end to their illicit activity.”

According to court documents, ChipMixer – one of the most widely used mixers to launder criminally-derived funds – allowed customers to deposit bitcoin, which ChipMixer then mixed with other ChipMixer users’ bitcoin, commingling the funds in a way that made it difficult for law enforcement or regulators to trace the transactions. As detailed in the complaint, ChipMixer offered numerous features to enhance its criminal customers’ anonymity. ChipMixer had a clearnet web domain but operated primarily as a Tor hidden service, concealing the operating location of its servers to prevent seizure by law enforcement. ChipMixer serviced many customers in the United States, but did not register with the U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) and did not collect identifying information about its customers.

As alleged in the complaint, ChipMixer attracted a significant criminal clientele and became indispensable in obfuscating and laundering funds from multiple criminal schemes. Between August 2017 and March 2023, ChipMixer processed:

- \$17 million in bitcoin for criminals connected to approximately 37 ransomware strains, including Sodinokibi, Mamba and Suncrypt;
- Over \$700 million in bitcoin associated with wallets designated as stolen funds, including those related to heists by North Korean cyber actors from Axie Infinity’s Ronin Bridge and Harmony’s Horizon Bridge in 2022 and 2020, respectively;
- More than \$200 million in bitcoin associated either directly or through intermediaries with darknet markets, including more than \$60 million in bitcoin processed on behalf of customers of Hydra Market, the largest and longest running darknet market in the world until its April 2022 shutdown by U.S. and German law enforcement;
- More than \$35 million in bitcoin associated either directly or through intermediaries with “fraud shops,” which are used by criminals to buy and sell stolen credit cards, hacked account credentials and data stolen through network intrusions; and

- Bitcoin used by the Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center, military unit 26165 (aka APT 28) to purchase infrastructure for the Drovorub malware, which was first disclosed in a joint cybersecurity advisory released by the FBI and National Security Agency in August 2020.

Beginning in and around August 2017, as alleged in the complaint, Nguyễn created and operated the online infrastructure used by ChipMixer and promoted ChipMixer's services online. Nguyễn registered domain names, procured hosting services and paid for the services used to run ChipMixer through the use of identity theft, pseudonyms, and anonymous email providers. In online posts, Nguyễn publicly derided efforts to curtail money laundering, posting in reference to anti-money laundering (AML) and know-your-customer (KYC) legal requirements that "AML/KYC is a sellout to the banks and governments," advising customers "please do not use AML/KYC exchanges" and instructing them how to use ChipMixer to evade reporting requirements.

"ChipMixer facilitated the laundering of cryptocurrency, specifically Bitcoin, on a vast international scale, abetting nefarious actors and criminals of all kinds in evading detection," said U.S. Attorney Jacqueline C. Romero for the Eastern District of Pennsylvania. "Platforms like ChipMixer, which are designed to conceal the sources and destinations of staggering amounts of criminal proceeds, undermine the public's confidence in cryptocurrencies and blockchain technology. We thank all our partners at home and abroad for their hard work in this case. Together, we cannot and will not allow criminals' exploitation of technology to threaten our national and economic security."

"Criminals have long sought to launder the proceeds of their illegal activity through various means," said Special Agent in Charge Jacqueline Maguire of the FBI Philadelphia Field Office. "Technology has changed the game, though, with a site like ChipMixer and facilitator like Nguyen enabling bad actors to do so on a grand scale with ease. In response, the FBI continues to evolve in the ways we 'follow the money' of illegal enterprise, employing all the tools and techniques at our disposal and drawing on our strong partnerships at home and around the globe. As a result, there's now one less option for criminals worldwide to launder their dirty money."


"Together, with our international partners at HSI The Hague, we are firmly committed to identifying and investigating cyber criminals who pose a serious threat to our economic security by laundering billions of dollars' worth of cryptocurrency under the misguided anonymity of the darknet," said Special Agent in Charge Scott Brown of Homeland Securities Investigations (HSI) Arizona. "HSI Arizona could not be more proud to work alongside every agent involved in this complex international case. We thank all our domestic and international partners for their support."

Nguyễn is charged with operating an unlicensed money transmitting business, money laundering and identity theft. If convicted, he faces a maximum penalty of 40 years in prison.

The FBI, HSI Phoenix and HSI The Hague investigated the case.

The U.S. Attorney's Office for the Eastern District of Pennsylvania is prosecuting the case.

German law enforcement authorities took separate actions today under its authorities. The FBI's Legal Attaché in Germany, the HSI office in The Hague, the HSI Cyber Crimes Center, the Justice Department's Office of International Affairs and National Cryptocurrency Enforcement Team, EUROPOL, the Polish Cyber Police (Centralnego Biura Zwalczenia Cyberprzestępczości) and Zurich State Police (Kantonspolizei Zürich) provided assistance in this case.

To report information about ChipMixer and its operators visit [rfj.tips/Duhsup](https://rfj.tips/Duhsup)  .

*A criminal complaint is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.*

Updated March 15, 2023

---

### **Attachment**

Complaint.pdf [PDF, 2 MB]

### **Topic**

Cybercrime

Press Release Number: 23-289