How cryptomixers allow cybercriminals to clean their ransoms

A thorough understanding of the operational underpinnings of these mixing services is key to comprehending how criminals are launder ransoms.

Nov 16, 2021

Cryptocurrency is a cybercriminal's best friend.

Actors all over the world have leveraged this technology's increased anonymity to buy and sell illegal goods, services, stolen data, underground infrastructure and force victims to pay ransom. While blockchain analysis enables researchers and law enforcement to glean information from illicit transactions, criminals have countered by adopting the use of cryptomixers to obscure their transactions and further complicate investigations. Intel 471 has observed actors in the cybercriminal underground relying on cryptomixing services to obfuscate the origin of their criminal earnings.

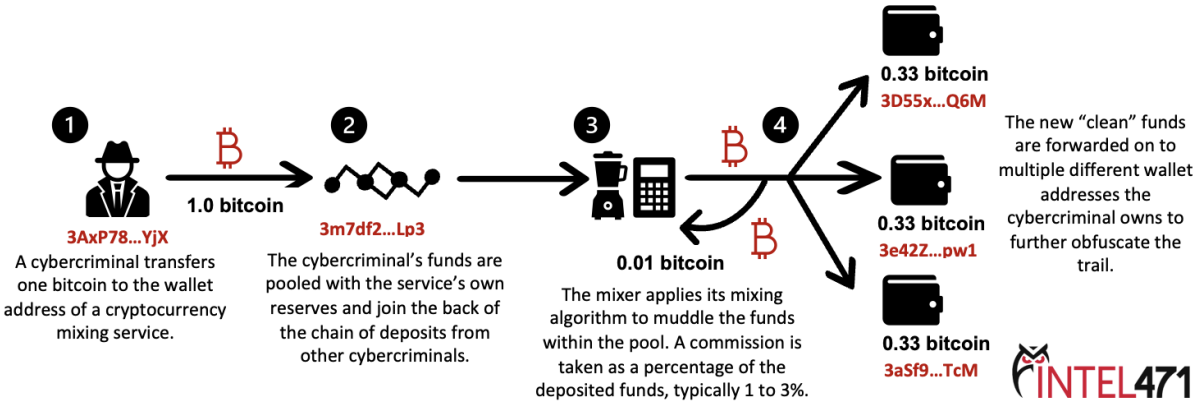
HOW MIXERS WORK

Cryptomixers are often stand-alone services that are available to the general public via the open internet. They often use anonymous means of communication and do not keep logs of customer transactions, which given the push by law enforcement for crypto exchanges to incorporate financial compliance laws into their operations, makes cryptomixers a useful tool for criminals.

Mixers work by allowing threat actors to send a sum of cryptocurrency, usually bitcoin, to a wallet address the mixing service operator owns. This sum joins a pool of the service provider's own bitcoins, as well as other cybercriminals using the service. The initial threat actor's cryptocurrency joins the back of

the "chain" and the threat actor receives a unique reference number known as a "mixing code" for deposited funds. This code ensures the actor does not get back their own "dirty" funds that theoretically could be linked to their operations. The threat actor then receives the same sum of bitcoins from the mixer's pool, muddled using the service's proprietary algorithm, minus a service fee. For added anonymity, the threat actor can choose to send this new "clean" sum of bitcoins to numerous wallet addresses to further obfuscate the trail of the illicit funds. This makes it more difficult for law enforcement to associate the original "dirty" cryptocurrency with the threat actor.

The diagram below further explains how this scheme operates:



POPULAR CRYPTOMIXERS

While the act of "mixing" cryptocurrency is not itself an illegal practice, these platforms aren't widely used by the vast majority of crypto-enthusiasts. Most users do not need the extra level of privacy nor want to lose crypto to the service fees that come with mixing cryptocurrency. The cryptomixers that Intel 471 observed all had well-established presences on multiple, well-known cybercrime forums. All of the mixers had professional-looking sites, likely serving as an attempt to make their operations appear more legitimate and attract a wider range of clients. None of the providers advertised their roles in money laundering, instead preferring to suggest their sites serve businesses using cryptocurrencies and individuals interested in protecting their privacy.

Among the most popular mixers observed by Intel 471 are:

- Absolutio
- AudiA6
- Blender
- Mix-btc

All the mixers Intel 471 observed were operational on the clear web and Tor network except mix-btc, which was only available on the open internet. All four providers offered their services in English, with Absolutio, AudiA6 and mix-btc also featuring Russian-language versions of their sites. All four mixers offered services for Bitcoin, while others also offered mixing services for Bitcoin Cash, Bitcoin SV, Dash, Ethereum, Ethereum Classic, Litecoin, Monero and Tether cryptocurrencies.

All the mixers listed a minimum balance for mixing services, which varied from 0.001 bitcoin (about US $60) for Blender to 0.006 bitcoin (about US $375) for mix-btc. Maximum amounts varied significantly, with Absolutio limited to 2 bitcoins (about US $125,700), Audi A6 to 27 bitcoins (about US $1.7 million) and Blender to 2,600 bitcoins (about US $163 million). Mix-btc did not specify an upper limit for transactions.

Additionally, all four mixers charge transaction fees, collected as a percentage of the total amount of cryptocurrency to be mixed. Some services allow users to choose a “dynamic” service fee, which is most likely done to complicate investigations into illicit cryptocurrency funds by altering the amount being laundered at different stages of the process, making it more difficult to tie the funds to a specific crime or individual. The fees are the following:

- Absolutio: Users select “dynamic” service fees, falls between 1 percent to 30 percent
- AudiA6: Flat service fee between 3 percent and 5.5 percent
- Blender: Users select “dynamic” service fee, falls between 0.6 and 2.5 percent

- Mix-btc: Flat service fee between 3 percent and 5.5 percent, additional charges depending on the volatility of bitcoin price

While these mixers do not share their wallet addresses publicly, Intel 471 found a wallet that was used by Blender from June 2020 to July 2020, handling bitcoin transactions in excess of 54 bitcoins (about US $3.4 million). Assuming an average transaction fee of 1.6 percent, this wallet could have received fees in excess of US $50,000 during that time period.

EVEN MORE "PRIVACY"

With RaaS groups wanting as many ways as possible to keep a low profile, some developers decided to integrate cryptocurrency mixing services in their administrative panel instead of relying on the web-based options. The developers behind Avaddon, DarkSide 2.0 (also known as BlackMatter) and REvil likely integrated the BitMix cryptocurrency mixer to facilitate the laundering of ransom payments for program affiliates. Additionally, BitMix itself operated an affiliate-type program in which registered partners received 50 percent of fees charged for mixing funds. This meant any RaaS groups engaged in this partnership would receive 50 percent of the commission BitMix charged ransomware affiliates With BitMix commissions reaching as much as 4 percent, the affiliate program presents an appealing prospect to RaaS groups.

CONCLUSION

Cryptomixers are a linchpin in ransomware schemes. Through these services, threat actors can achieve their end goal of cashing out and keeping the criminal underground liquid through the trade of illicit goods and services. A thorough understanding of the operational underpinnings of these mixing services is key to comprehending how criminals are laundering the money they earn from their crimes. It's important to understand how all facets of a ransomware operation works if civil society is to stop the losses inflicted by these schemes.