EUROPOL
EC3 | European Cybercrime Centre

The Hague, April 2020

Intelligence Notification No 08/2020

CYBER BITS
Series: Knowledge

Wasabi Wallet – Part I: Introduction

What happened?

In the last period, Europol's EC3 started to notice an increasing number of investigations involving Wasabi Wallet. Wasabi is a light wallet that implemented a very effective method of mixing bitcoin using a so-called "coinjoin". This means that it merges coins originating from different users into one transaction and redistributes these into many standardised amounts on the output side, which makes it difficult to correctly link inputs with their respective outputs.

Image source: https://bitcoinmagazine.com/

Wasabi claims to be an open source, non-custodial, privacy-focused Bitcoin wallet for desktop use, which implements trustless coin shuffling with mathematically provable anonymity.

How does it work?

Let's take a closer look at the abovementioned four adjectives:

Open-source: Same as many other wallets including the very first one - Bitcoin Core – all have code transparently showcased at GitHub so that everyone can check that the code is not doing anything malicious.

Non-custodial: Users who download the wallet store all bitcoins locally, so the administrators and developers of Wasabi have no way of accessing a user's balance or funds.

This also means that the AML (anti-money laundering) legislation including Europe's latest AMLD5 (the 5th Anti-Money Laundering Directive) does not apply to this service.

Privacy-focused: Unlike most other cryptocurrency wallets, the main purpose of Wasabi is to protect the anonymity of its users – via non-optional use of passwords, integration of TOR and, most importantly, its unique and elaborate coin mixing mechanism.

Additional privacy-focused transaction-specific features include:
- Very large transactions mixing funds of many participants at the same time;
- Blind signatures that assure that even Wasabi operators cannot link inputs and outputs;
- Standardised randomised amounts;
- Generation of a new address for each incoming transaction;
- A coin control feature (gives users a choice on which input address to spend);
- Custom transaction fees;
- Block-filter.

EC3 Cyber Intelligence Team O31@europol.europa.eu PGP Fingerprint: C91D 6329 B144 4F38 E038 288E 2FF8 3886 021D 47DF

The last item deserves a more elaborate technical explanation. If a user runs a light wallet, such as Wasabi, that does not require storing the 250 GB bitcoin blockchain, the wallet needs to connect to one of the nodes in the bitcoin network to get the current status for all addresses in the wallet. However, this may decrease a user's privacy as the tracing companies operate many of the nodes in the network, who could then easily make a link between a wallet and all addresses it controls and correlate transactions with IP addresses.

To make this process less reliable, some wallets (e.g. Multibit or Bread) implemented so-called Bloom filters, which request many addresses from the node, including false negatives. However, this did not stop tracing companies from harvesting valuable information for their tools. Block-filter goes one step further than Bloom filters by downloading full blocks of data, making it difficult to establish which address in the block is actually being requested. This should prevent the tracing tools from linking bitcoin addresses to IP addresses and clustering addresses based on network traffic.

Trustless: When using centralised mixers, users run a risk of their funds being stolen by the mixer. Another risk is that the centralised service may be taken down by law enforcement who may seize logs and subsequently identify users behind the transactions. Wasabi completely mitigates the first risk as the user has a complete ownership of the private keys and while the wasabiwallet.io site could theoretically be taken down, IP logs would be worthless as the service uses TOR by default.

How popular is the service?

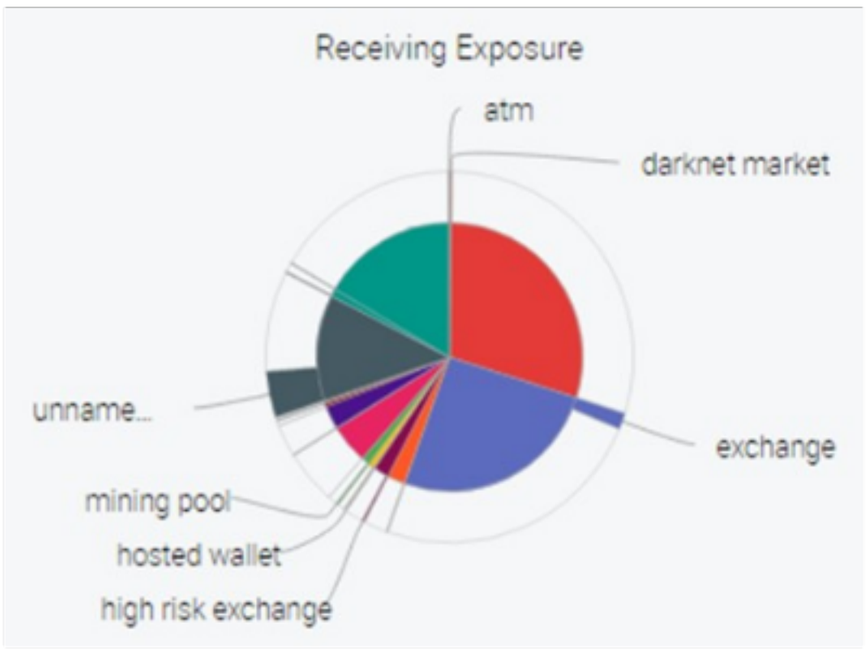
Certainly popular enough to spark our interest. Wasabi has been in operation from Autumn 2018 and has gradually been gaining traction. Looking at the Wasabi cluster in Chainalysis, the service received over 110,000 BTC, which corresponds to over €500 million as of March 18, 2020.

The ratio of addresses to transactions is very high, which is expected given multiple parties mixing their coins within the same transaction.

Chainalysis Name		Category	
WasabiWallet.io		mixing	
Balance:	165.512... BTC	Transfers:	134,397
Sent:	109,951.619... BTC	Withdrawals:	507,138
Received:	110,124.786... BTC	Deposits:	140,860
Total Fees:	7.654... BTC	Addresses:	814,573

How is the service used?

According to the same tool, over the last three weeks, BTC in the amount of nearly 50 million USD were deposited into Wasabi with almost 30% coming from dark web markets. This is a significant amount, relatively speaking, given the dark web transactions are estimated to have only 1% share of total transactions.



Why do you need to know?

- Wasabi is a very effective decentralised bitcoin mixer with many privacy-focused options;
- It provides possibly the most convenient and secure way to mix bitcoins;
- Wasabi became popular and naturally also attracted those involved in criminal activities;
- The next Cyber Bit will provide an insight into a hands-on interaction with Wasabi, demonstrating a transaction and explain the possibilities for law enforcement investigations. Spoiler alert: things are not looking good.

EC3 would welcome feedback on this note. Please fill in the form through the link below making reference to the Intelligence notification No. on top of this CyberBit: https://ec.europa.eu/eusurvey/runner/o31_report_feedback

EC3 Cyber Intelligence Team O31@europol.europa.eu PGP Fingerprint: C91D 6329 B144 4F38 E038 288E 2FF8 3886 021D 47DF

EUROPOL
EC3 | European Cybercrime Centre

The Hague, May 2020

Intelligence Notification No 10/2020

CYBER BITS
Series: Knowledge

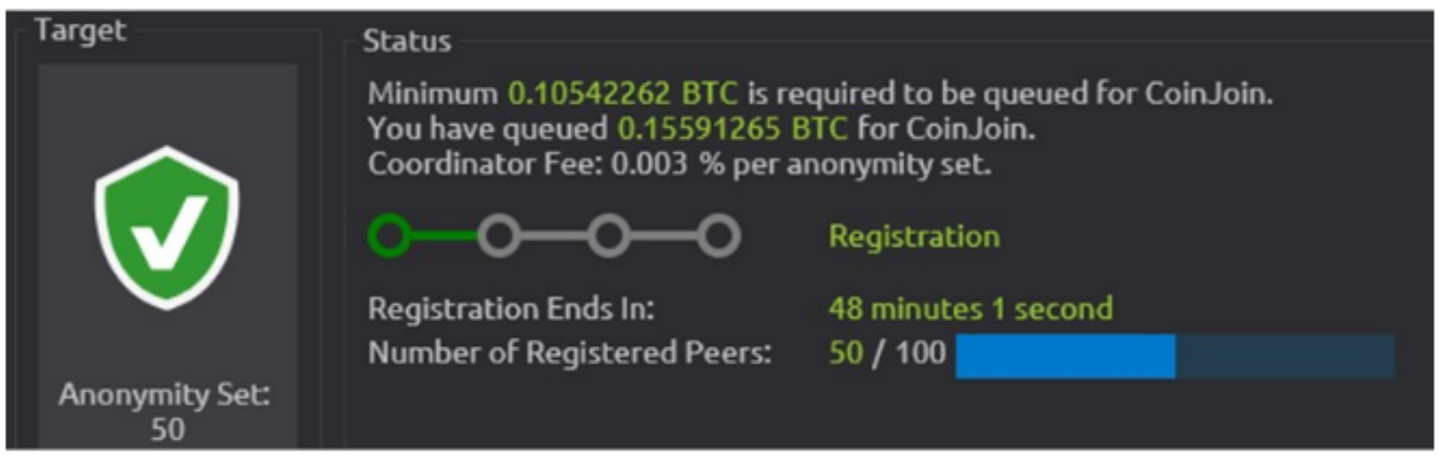
Wasabi Wallet – Part 2: Hands-On

What happened?

Due to an increasing number of cases featuring Wasabi Wallet, we released an overview of the topic in the first Cyber Bit released in April. This week, we focus on hands-on experience with the wallet, and include law enforcement-relevant considerations.

How does it work?

- After the user downloads and installs the Wasabi desktop application, the application will generate a deposit address. The user then sends his tainted bitcoins into this address and once the funds arrive, he may start the mixing process, which can easily take over one hour:



After the mixing is over, the user receives mixed funds into a completely different bitcoin address and can then send the funds further – either to the user's own wallet or to any other wallet out there.

What does the transaction look like in the blockchain?

We deposited 0.15591265 BTC into our Wasabi address. You may notice the wallet uses a so-called Bech32 address format starting with "bc1". This is an address format used for all Wasabi addresses, so when the mixing takes place, the transaction will have a very distinct pattern. In total, there were 72 inputs and 108 outputs, of which only the first 5 rows are shown here:

EC3 Cyber Intelligence Team O31@europol.europa.eu PGP Fingerprint: C91D 6329 B144 4F38 E038 288E 2FF8 3886 021D 47DF

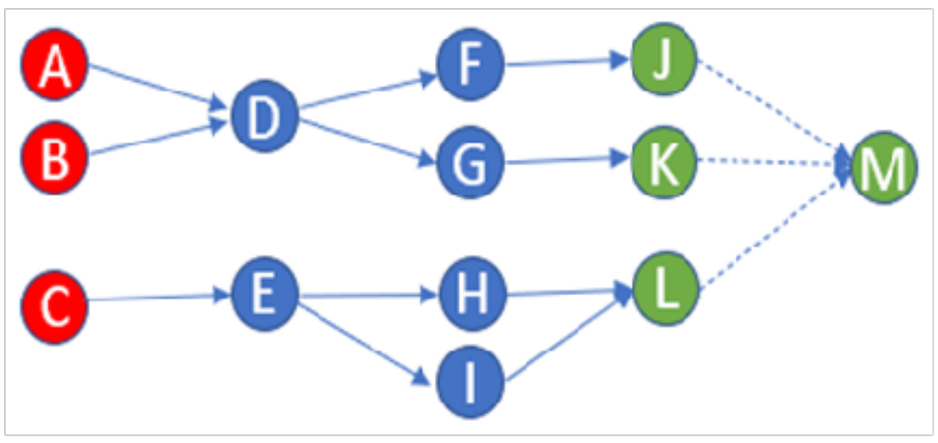
CYBER BITS
Series: Knowledge

Wasabi transactions of similar size are very common. Yet another pattern of Wasabi transactions are the amounts – which are sorted from lowest to highest amount and many of the amounts on the output side are repeated. Looking at the abovementioned transaction with 108 outputs, the amount 0.10547236 is repeated 49 times, while 0.21063776 appears 10 times. In other transactions, we can often see that amounts of 0.1xxx, 0.2xxx or 0.4xxx are used, where the higher denomination approximately corresponds to double the amount of the smaller denomination.

There is a large number of similar transactions in the bitcoin blockchain that bundle multiple inputs and outputs. This is a common occurrence with services. For example, cryptocurrency exchanges may try to facilitate withdrawals of multiple customers packed within one transaction. We can, however, still distinguish these transactions, as the output side of exchange withdrawals features different address formats used by individual clients. The amounts will not be sorted and will not be repetitive and will have a higher occurrence of round numbers (such as 0.5 BTC).

Looking at a sample of 500 addresses that received funds a week ago, Chainalysis identified about 80% of these correctly as Wasabi addresses. So, if your suspect is consistently using the mixer, the commercial tools available should be able to pick it up - but being able to visually identify Wasabi transactions may still prove to be useful.

Can Wasabi transactions be demixed?
Realistically speaking, in most cases the answer is negative. The sheer amount of transactions and uniform output amounts, typically offer too many options of where the funds could have moved. Still, there may be a glimpse of hope if the suspect makes a mistake and decides to group the mixed coins together as suggested by the following scenario:

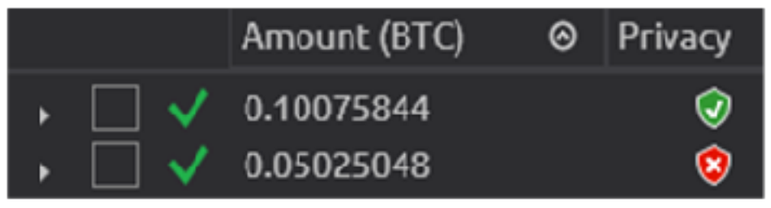


Addresses A, B and C store BTC originating from criminal activity. BTC are sent to Wasabi wallet deposit addresses D and E and after mixing end up on F, G, H and I.

Later on, suspect withdraws these to his "clean" addresses J, K and L but may make a mistake of sending all funds to the same address or wallet M.

Using "what-goes-in-must-go-out" logic, the amount received on M would correspond to the values stored on Addresses A, B and C, albeit slightly lowered by transaction and mixing fees, which would allow manual demixing of the transactions. Naturally, if the suspect is careful and splits proceeds from addresses J, K and L among separate wallets without any consolidation taking place later on, this technique will not work.

Theoretically, the investigator can also assume that if the suspect sends for example 0.15x BTC into Wasabi and only 0.1x BTC is mixed as one of the standardised output amounts, a change that can be calculated might be traced. However, Wasabi takes this into account and clearly alerts the suspect that the change address was not properly mixed:



Note that this cyberbit reflects the current level of knowledge and that in future there may be a better solution of analysing and possibly demixing Wasabi transactions. Unlike centralised mixers that operate as a blackbox, all Wasabi transactions are transparently stored in the blockchain for tracing tool companies and LE to analyse. Dutch FIOD (Fiscale Inlichtingen en OpsporingsDienst) has started promising technical research into behaviour and demixing of Wasabi transactions and are interested in hearing about similar research activities in other countries.

Why should you know?

- It is easy to visually identify Wasabi wallet transactions just by looking at them in the blockchain;
- Tracing tools will identify most of the addresses but will not demix the transactions;
- It may be possible to follow the money if the suspect happens to make a mistake ;
- Suspects who avoid major slip-ups have a very high probability of staying undetected;
- If you or your colleagues actively research Wasabi or other mixing - do get in touch!

EC3 would welcome feedback on this note. Please fill in the form through the link below making reference to the Intelligence notification No. on top of this CyberBit: https://ec.europa.eu/eusurvey/runner/o31_report_feedback

EC3 Cyber Intelligence Team O31@europol.europa.eu PGP Fingerprint: C91D 6329 B144 4F38 E038 288E 2FF8 3886 021D 47DF