The Hague, 12/12/2017

The use of Virtual Currencies for Terrorism Financing purposes

Europol – Financial Intelligence Group

Document Reference [#936623]

Risk Analysis

Europol Public Information

Table of Contents

1 BACKGROUND 3

2 CONTEXT 3

3 LEVEL OF THREAT 4

4 LEVEL OF VULNERABILITY 9

5 LEVEL OF RISK 10

6 MITIGATING MEASURES 11

1 BACKGROUND

On July 2017 Europol was tasked by the European Commission to carry out a risk analysis on the use of virtual currencies in the area of financing terrorism. Such document was concluded and delivered in August 2017. That risk analysis generated a positive feedback and Europol was requested to prepare a public document based on it to be shared with experts, think tanks and academia and thus generate the necessary awareness. This is the outcome.

2 CONTEXT

Virtual currencies (VCs) are commonly traded on the internet and are generally characterised by non-face-to-face customer relationships. Decentralised convertible VCs permit pseudonymous (some cryptocurrencies[1] permit even anonymous) usage, and are therefore being used by criminals and terrorist financiers to cross borders with value, transfer funds or for the purchase of goods and services.

Furthermore, looking for example at Bitcoin (a pseudonymous VC), the wallets, addresses and transactions are not tied to the identity of the user. Only by use of advanced financial investigative techniques can such user be identified. By using TOR network or other methods to mask IP addresses criminals and terrorist financiers can make it even more difficult to determine where their transactions originated from. Other anonymity enhancers commonly used by criminals (and potentially by terrorist financiers) are mixers and peer-to-peer traders.

[1] E.g. Monero, Zcash, Dash.

3 LEVEL OF THREAT

While VCs have gained popularity due to their key characteristics such as global availability, ease of access, reliable and irreversible transactions, low cost and high speed for international movements/transfers, their expansion among Terrorist Organizations (TO) seems to be slow and has not yet matched the pace of transnational Organized Crime Groups (OCGs), especially those involved in cybercrime.

The number of known/identified cases of VCs related to terrorism financing remains very low. Currently only a small number of incidents are known involving the usage of VCs by terrorist groups, lone wolf actors, associates and financiers of TO. These few cases, some of them stemming from public sources, mostly relate to fundraising activities via social media usually advertised on the dark web and abusing pre-established crowdfunding networks and web based services. Such cases were only able to obtain small amounts of VCs.

Case example A:
In July 2015 the media wing of the Mujahideen Shura Council in the Environs of Jerusalem - an assembly of Salafi-jihadist groups in Gaza - ran a social media fundraising campaign. By June 2016 the option for donors to pay in Bitcoins was added and as of August 2016 the campaign had received roughly 0.929 bitcoins (around €470) via two transactions, despite seeking at least $2,500 per fighter.[2]

[2] https://www.thecipherbrief.com/column/private-sector/new-frontier-terror-fundraising-bitcoin-1089

Case example B:

In early 2015 a researcher claimed to have concrete evidence linking an Islamic State (IS) cell based in the United States to a Bitcoin fundraising event on the dark web. The researcher came across the fundraising site through a closed Turkish forum. The fundraising activity was carried on the dark web and only accepted Bitcoin donations. The fundraiser managed to raise five Bitcoins (approximately €940) before the FBI shut down his account.[3]

Isis uses bitcoin for fundraising and supporting US-based terror cells 'on both coasts'

By Anthony Cuthbertson
Updated

MORE

Isis, shown here before the execution of 13 men in Iraq, is reportedly using bitcoin to fund jihadist cells in the US (Twitter)

Moreover in case examples A and B it was not established if the funds were indeed used or intended to be used for the terrorism financing purposes, or if they were just scams/frauds. In addition some press releases[4] indicate cases where donors are instructed via social media (including twitter), internet forums or in the dark web on how to use Bitcoins so that they can provide untraceable financial support to terrorist organisations such as IS.

[3] http://www.ibtimes.co.uk/isis-uses-bitcoin-fundraising-supporting-us-based-terror-cells-1485670

[4] https://www.justice.gov/opa/pr/virginia-teen-pleads-guilty-providing-material-support-isil
https://www.washingtonpost.com/news/worldviews/wp/2015/06/09/the-islamic-state-or-someone-pretending-to-be-it-is-trying-to-raise-funds-using-bitcoin/?utm_term=.ff5182890393

Case example C:

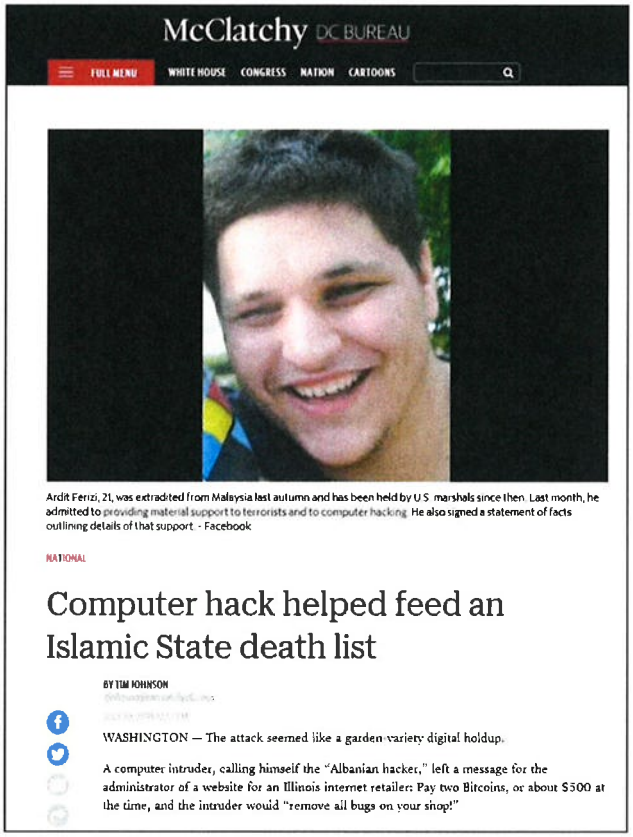
Recently Indonesia's financial-transactions agency announced[5] that Bitcoin and online payment services were used by Islamic militants in the Middle East to transfer funds to Indonesia where they were used to finance terrorist activities. Such cases more than doubled from 12 in 2015 to 25 in 2016.

As bitcoin and other cryptocurrencies become adopted by society at large we will see this payment method being abused by those who may want to take advantage of some of the key cryptocurrencies features (like the ease to cross borders with value and to transfer funds) to facilitate terrorist activities.

[5] http://www.straitstimes.com/asia/se-asia/militant-bahrun-naim-used-paypal-bitcoin-to-transfer-funds-for-terror-attacks-in?utm_campaign=Echobox&utm_medium=Social&utm_source=Facebook&xtor=CS1-10#link_time=1483941796

Case example D:

In August 2015, a computer hacker with ties to IS called "Albanian hacker" installed malware on the server of a private US company to illegally obtain data that allowed him to create a "hit list" for IS containing the identities of 1.351 U.S. government and military personnel. This hacker later demanded the payment of two Bitcoins from the private company to remove the installed malware.[6]



McClatchy DC BUREAU

FULL MENU WHITE HOUSE CONGRESS NATION CARTOONS

Ardit Ferizi, 21, was extradited from Malaysia last autumn and has been held by U.S. marshals since then. Last month, he admitted to providing material support to terrorists and to computer hacking. He also signed a statement of facts outlining details of that support. - Facebook

NATIONAL

Computer hack helped feed an Islamic State death list

BY TIM JOHNSON

WASHINGTON — The attack seemed like a garden-variety digital holdup.

A computer intruder, calling himself the "Albanian hacker," left a message for the administrator of a website for an Illinois internet retailer: Pay two Bitcoins, or about $500 at the time, and the intruder would "remove all bugs on your shop!"

[6] http://www.mcclatchydc.com/news/nation-world/national/article90782637.html

Case analysis results:

Most of the case examples demonstrate that TOs are most probably already using VCs to move value, facilitate international transfers and for the purchase of goods and services through the internet.

But they also demonstrate that TOs have not yet adopted VCs on a large scale, the reasons for that are probably the following:

a) Most TOs lack the degree of knowledge and technological sophistication needed to use VCs.
b) TOs are probably not comfortable with the high volatility in value[7] of VCs.
c) Most TOs operate in cash intensive economies were the acceptance of VCs is very limited to non-existent. Thus they need fiat currency to operate.
   The need to exchange cash for VCs and VCs for cash introduces a layer of complexity and of increased vulnerability that TOs are not always willing to take.
d) The VC that has achieved the greatest market capitalization and penetration – Bitcoin – is not completely anonymous, but only pseudonymous. The cryptographic addresses of the sender and the recipient of transactions are recorded in the blockchain - the publicly accessible ledger; although they are not linked to real-life identities, with enough investigative resources it is possible to uncover the true identity of the senders and recipients of Bitcoin transactions.

However this limited number of cases is likely to increase as VCs grow in increased anonymity, in greater market acceptance and in a more user friendly technology. Work is also underway to obfuscate even more true identity of the users/owners of cryptocurrencies. A number of new developments dedicated to increase anonymity levels, both in terms of new virtual currencies and on new technologies, are already in use.

Criminals are making use of new cryptocurrencies such as Monero and Dash because of their enhanced anonymity properties (by combining multiple transactions, hiding the amount of each transaction and obscuring the origin and recipient of funds). Terrorist financers are expected to follow these steps.

Similarly, Dark Wallets seek to anonymize Bitcoin transactions. They disrupt the blockchain's potential to identify suspects by combining random contemporaneous transactions and then encrypting recipients' information so that it will not appear on the blockchain.

Hardware and E-wallets are also becoming more sophisticated with plausible deniability mechanisms being added. Plausible deniability is a feature that allows for the creation of hidden wallets attached to visible ones.

---

[7] In May 2017 a dispute among developers about one of the technical characteristics of the virtual currency among other things led to a 20 percent decline in the value of Bitcoin over a single weekend. For more information: https://www.cnbc.com/2017/05/29/bitcoin-correction-price-value.html

Likewise, more customizable, white-label services have entered the market, supplying both software and infrastructure to individuals interested in creating their own VC exchanger. The proliferation of unregulated VCs exchangers could further spread TF/ML risks, by giving criminals easier access to the exchange of virtual currencies for fiat currency, without undergoing appropriate CDD or STR reporting obligations.

Conclusion: Information was gathered demonstrating that suspects are probably already using VC to finance terrorist activities. However, the use of VC requires technical expertise, reliable telecommunication networks and internet services which are not present in many of the areas where TOs operate. Some current key characteristics of VCs make it less attractive for TOs. Consequently, the level of TF threat related to virtual currencies is considered as moderately significant (level 2).

4 LEVEL OF VULNERABILITY

The most important element of vulnerability for VCs is not only the fact that they are not regulated under a common EU framework but also the fact that some of them (the decentralized VCs) cannot even be regulated under the traditional framework.

Decentralized currency systems neither have a central server nor a central supervisory body which means there is no one monitoring the transactions and identifying suspicious transactions exchanged among peers or non-compliant entities.

The assessment of the TF vulnerability related to VCs will thus take into account the fact that, currently, they are not yet regulated in the EU and that the risks of their misuse for TF purposes is already emerging.

a) **Legal framework**
   The lack of a harmonized legal framework is the most important vulnerability. In the current situation, VC exchangers, wallet and ATM providers cannot be monitored and supervised in the EU within a harmonized manner. There are no common rules to ensure that these key players will apply AML/CFT requirements. Due to a general willingness of partners from the private sector, national/international cooperation between VC exchangers and LEAs/FIUs exists, but it's done in a voluntary and informal manner.
b) **Exposure:**
   VCs permit to conduct rapid transactions without disclosing the true identity of their users/owners. Given that they are provided through the internet the cross-border element is a prevailing one, thus increasing the risk of interaction with high risk customers and high risk areas. It is nevertheless important to mention that being a developing technology requiring IT skills and expertise, VC are not easy to use and the number of transactions suspected to be connected to TF are still low.

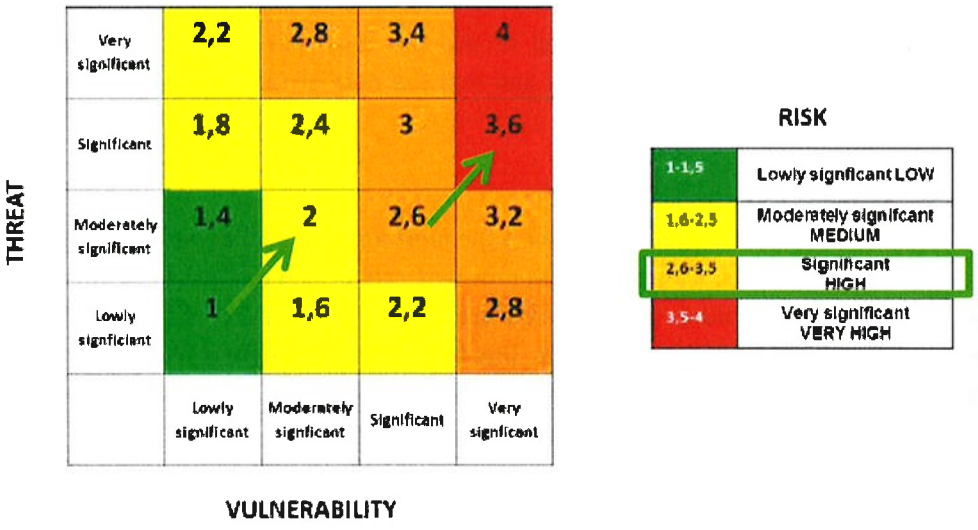
c) **Awareness:**

The exact component of the TF vulnerability is difficult to assess in a comprehensive manner due to the fact that VC exchangers, wallet and ATM providers are not regulated as obliged entities under the EU AML/TF Directive[8]. As it currently stands some VCs service providers such as exchangers do fill suspicious transaction reports but on a scattered and voluntary basis. It is for this reason assumed that their level of awareness to TF risks is low.

Conclusions: The most important element of vulnerability for virtual currencies providers is the fact that they are not yet regulated in the EU (and some cannot even be regulated under the traditional framework). Currently they are not being properly monitored, no proper CDD is being conducted nor consistent Suspicious Transaction Reports are being filled with FIUs. The inherent risk exposure is also very high due to their inherent nature (internet, cross-border and anonymity possibilities). Consequently, the level of TF vulnerabilities related to virtual currencies is considered as significant/very significant (level 3 to 4 =3,5).

5 LEVEL OF RISK

Based on the levels of threat and vulnerability previously explained and similarly to the EU-COM Supra National Risk Assessment of money laundering and terrorist financing risks one can determine that the risk level on the use of virtual currencies for terrorism financing purposes is 2,9 = (2x 40%) + (((3+4):2) x 60%). A 2,9 risk level corresponds to a significant risk, which is the lowest form of high risk.



[8] In July 2016 the European Commission proposed Directive amending the 4th AMLD, currently under discussion (see Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, 2016/0208 (COD), 05.07.2016, European Commission, p. 10).

6 MITIGATING MEASURES

The Commission already submitted in its proposal for amending the 4AMLD Directive (UE) 2015/849 that virtual currency exchange platforms as well as custodian wallet providers should be added to the list of obliged entities under the now soon to become 5AMLD.

Even if doubts currently exist if this amendment will cover or not VC ATM providers, the fact is that once the 5AMLD comes into force, the current vulnerability level will somewhat decrease.

Moreover a good understanding of VCs is of the utmost importance to detect its usage for TF purposes. It is therefore necessary that all EU CT investigative units provide training, promote expertise and practical knowledge to their experts on TF on the tools and investigative techniques needed to understand, identify and monitor the use of new payment systems, including VCs.

Nonetheless, the growing trends of internet-based radicalization of lone wolf terrorist plotters and of EU based terrorist financers as well as the natural evolution of VCs to become more user-friendly, more widely accepted and with stronger anonymity characteristics - all will necessary lead to an increase in their usage for TF.

This eminent threat demonstrates the pan-European need of supplementary financial intelligence in general and for terrorist financing in particular. Such initiatives should permit to detect, prevent and investigate red flag indicators, leads and high value targets, making sure all pieces of financial intelligence in the EU could be timely available to those in need on the fight against terrorism. Thus to mirror such threat in its changing nature and level of gravity the launch of new international public/private partnerships/initiatives should be strongly considered.