Crime and online anonymous markets
Pieter Hartel, Rolf van Wegberg, Delft University of Technology

Introduction

Online anonymous markets have been around since early 2011 and are a prominent part of today’s cybercrime ecosystem. Their popularity as markets in illicit goods has steadily grown over the years [Soska2015]. With the rise of markets like Silk Road, similar marketplaces came into existence where next to drugs, supply and demand of other products and services could meet: ranging from physical goods, like passports and weapons, to digital goods and services, like carding and cybercrime software [Aldridge2014; Thomas 2015]. As a result we can witness an increasing supply of criminal product and services on standardized digital trading platforms in the underground economy [Thomas2015].

The general public has become aware of online anonymous markets and their underlying technologies, such as The Onion Router (TOR) and Bitcoin, by their practical application. Bitcoin handles transactions ‘anonymously’ and the TOR-protocol supports ‘anonymous’ browsing. We use inverted comma’s to indicate that both these technologies offer a degree of anonymity that, given enough effort, can always be broken. The perception of anonymity attracted large number of vendors and buyers to online anonymous markets. Over the last few years, these have further matured in business continuity management, in consumer-oriented operations, and in turnover. A single top tier market can turn over around 200,000 US dollars daily [Soska2015]. But how do these online anonymous markets change criminal behaviour and what type of criminal justice approach suits this development?

The focus of traditional law enforcement interventions lies primarily in arresting, prosecuting and seizing drugs on anonymous online markets. According to international agencies such as Interpol, these strategies have only limited success and traditional interventions may actually promote innovation and evolution of the online anonymous markets. On top of that, widely publicized court cases provide online anonymous markets with free advertisement [Decary-Hetu2017]. Ironically, the anonymous or pseudonymous nature of these markets – provided by technologies such as TOR and Bitcoin - creates a high level of transparency of the entire ecosystem of markets, giving LEA the opportunity to shift their policing efforts based on ecosystem insights. Hence, interventions can focus on disrupting the ecosystem and the business models behind the online anonymous markets. As the current criminal justice interventions have proven to be relatively ineffective, we look at how the criminal justice approach to crime on online markets can lever these technical components in novel interventions – making use of the transparent ecosystem.
We begin by defining a few key concepts. Then we describe the two key technologies (TOR, Bitcoin) that made online anonymous markets possible. We also discuss the genesis of one of the early online anonymous markets (Silk Road). Then, we discuss some of the mistakes that have been made in operating dark markets that could be leveraged for effective police interventions.

Definitions
We begin by giving some definitions:

- An anonymity network is network overlaid on the Internet that supports reasonably anonymous communication between parties.
- A crypto currency is a cryptographic software based currency that can be traded reasonably anonymously.
- The surface web is the portion of the Web that is readily available to the general public and searchable with standard web search engines.
- The deep web is the portion of the Web whose contents are not indexed by standard web search engines for any reason.
- An online anonymous market is a market place where anonymous parties trade goods and services online.

The TOR network
TOR is one of the most popular anonymity networks [Li2013b]. Clients and services can interact whilst enjoying strong anonymity. TOR anonymity protects political activists and embedded journalists but also terrorists and paedophiles.

The TOR network is accessed via special browser (The TOR browser) that can be downloaded free on the Internet. The web servers on the TOR network are so called hidden servers that can only be accesses using the TOR browser.

A few thousand volunteers, mostly in the US and Western Europe make their computers and network connections available to run the TOR network [Li2013b]. These volunteers are essential to provide the anonymity on the TOR network because every connection is routed via the computers of a number of randomly chosen volunteers. If the ‘volunteers’ decide to collude, the anonymity of the TOR network is completely compromised.

An in depth analysis [Guitton2013] of the offerings of three hidden service directories covering 1,171 hidden services shows that the largest category, with 18% of the offerings is devoted to child pornography, and that one of the smallest categories is devoted to politics, with 1%. About half of the bandwidth processed by the TOR network is used for BitTorrent traffic, which is typically used to circumvent anti-piracy laws.

There are some publicly available alternatives to TOR. For example the I2P anonymity network, which has a similar design as TOR, as well as a similar user base, and Anonymizer [Li2013b]. Botnets can also be used as anonymity networks. There are many more and much larger Botnets than the TOR network.
The Bitcoin network

Crypto currencies, such as Bitcoin rely on public and private keys, and digitally signed transactions. Every signed transaction is recorded in a data structure called the blockchain. This is a public ledger, which everyone can check. A network of mutually distrustful volunteers maintains the safety, and integrity of this public ledger.

The first open source Bitcoin client software was released in 2009. Initially only used by a small community, the knowledge and use of Bitcoin is now widespread, with several services such as ATM machines accepting BTC both online and offline. Bitcoin is legal tender in some countries.

Bitcoin supports pseudonymous payment, but not anonymous payment. Compared with numbered Swiss banking accounts, the Bitcoin address itself acts as a unique identifier and the account is only accessible by the owner who has the private key. Hence, Bitcoin addresses are not registered to individuals. Yet, all historic information on any Bitcoin address and transactional information are logged in the blockchain. In that sense, a Bitcoin address becomes a traceable pseudonym of its owner.

There are hundreds of crypto currencies but Bitcoin has the largest market capitalisation. Bitcoin can be bought and sold for fiat currency at exchanges. Many hold Bitcoin to speculate on exchange rate fluctuations, but Bitcoin is also used for illicit purposes. For example ransom ware demands are usually paid in Bitcoin. Some major corporations even hold Bitcoin to be able to give in to ransom demands.

Online anonymous markets

Different researchers have studied how online anonymous markets support the evolution of criminal activity in the underground economy. The first studies focused on underground forums, e.g. carding forums revolving around the (re)selling of stolen credit card details [Motoyama2011]. After the first standardized market came into existence, i.e. Silk Road, mostly computer scientists started to shift focus to look at these online anonymous markets [Soska2015]. Most existing studies include (or even focus on) drugs and physical goods, which represent a large share of the products offered on the markets.

Furthermore, social scientists investigated the increase in online drugs trade, specifically the wholesale side of Silk Road 1 drugs offerings, and what factors determine vendor success [Aldridge2014]. In addition to large-scale quantitative studies into the evolution of online anonymous markets, we can point to qualitative studies on buyers and sellers (vendors) on markets and forums. For instance, Van Buskirk et al. [Buskirk2016] specifically focused on the motivation of drug buyers in Australia to turn to online anonymous markets instead of street dealers. They found that a lower risk and higher quality of the drug are important.
Silk Road was one of the first online anonymous markets operating as a hidden service on the TOR network. It was the brainchild of a visionary libertarian entrepreneur who went astray. Ross Ulbricht created 'Silk Road' as a platform, where libertarian thoughts could be exchanged anonymously. Others, however, saw a vast business opportunity. From the start, Silk Road became a place where not only libertarians shared ideas, but also were people who would buy and sell illegal goods and services, mostly drugs. Knowing or unknowingly, Ulbricht kick started an underground market in illegal goods and services. In 2012 Silk Road had hundreds of sellers, mostly located in the US [Christin2013]. During its existence Silk Road was used by hundreds of thousand customers from across the world.

Silk Road mandated the use of Bitcoins for all financial transactions, thus providing relatively anonymous payment services. Today, other crypto currencies, like Monero, only have a marginal presence on anonymous online markets. For example an investigation into the payment options of 2017 market-leader AlphaBay shows that only 4% of all offerings accept another crypto currency than Bitcoin.

Silk Road used self-regulation mechanisms similar to those in use by most online markets to “keep honest people honest”. For example, Silk Road used a rating system for the buyers and an escrow facility for payments [Christin2013]. These self-regulation mechanisms ensure that the quality of the products higher than those available “on the street” and that the risk of non-delivery or non-payment is lower than on the street. Physical goods would be delivered via the postal system. The absence of physical contact between buyer and seller also means that there is less violence than on the street. This means that the user may be better off buying drugs from online markets than from the street [VanHout2014].

Silk Road is often described as a market for consumers, with a better range of products, better quality and less risk of violence than on the street. However, a detailed analysis of the prices and quantities sold suggests that about half the revenue on Silk Road is generated by business-to-business transactions [Aldridge2014].

Silk Road was taken down by the FBI in October 2013 and replaced within 37 days by new services, including Silk Road 2. Vendors are now trading on several markets simultaneously to improve their business continuity.

**Criminal justice approach to online anonymous markets**

Being confronted with new aspects of digital innovations in crime, law enforcement had to come up with at least the same level of innovation in their actions against these online anonymous markets. And they did. Law enforcement agencies around the world have intervened on online anonymous markets in three different ways. First, they set up interventions focusing on the ecosystem, such as affecting confidence in anonymous markets: creating distrust by infiltrating the market. Second, they aimed for interventions on specific markets,
such as making it unavailable by seizing computer servers. Thirdly, they tried to intervene on a personal level by unmasking the administrators, such as Ross Ulbricht. He is now serving a life sentence.

**Policing the Ecosystem**

Recently, during Operation Bayonet two leading online anonymous markets on the Dark Web took centre stage in a joint policing effort of the Federal Bureau of Investigation (FBI) and the National High Tech Crime and Dark Web unit of the Dutch Police. In a coordinated sweep, the FBI succeeded in the takeover and subsequently take-down of AlphaBay, while the Dutch Police took over, briefly managed, and then shut down Hansa Market. By planning these actions sequentially, the police agencies expected criminals active on AlphaBay to make their way to Hansa Market – which at that moment was operated by the Dutch Police. This put the police agencies in a perfect position to not only disrupt the ecosystem, but also to collect valuable data on thousands of users. This led to a string of arrests of large-scale vendors.

**Pulling the plug**

Operation Onymous was a coordinated operation between police forces from 17 countries coordinated by Europol in 2014. It resulted in the take down of over 50 sites. Reporters claim the true number lies closer to 27 different sites. Amongst others, Operation Onymous shut down the online anonymous markets Cloud 9, Hydra & Silk Road 2. Law enforcement arrested 17 persons, of which only one name has been made public: Blake Benthall, known on Silk Road 2 as the main administrator under the pseudonym ‘DEFCON’.

**Making it personal**

Next to interventions aimed at either the ecosystem or specific markets, there have been interventions at the personal level. This included interventions that actively informed people of the fact that, despite their assumption of being anonymous, they were identified by the law enforcement. In three different ways, these users were informed. First, lists of identified usernames and parts of their real name and residence were published on a website that is managed by the police on the DarkWeb. Secondly, a so-called ‘love letter’ informs identified persons. Thirdly, “knock-and-talk” actions were carried out, in which the police personally informed the persons behind certain usernames and identities.

**Measuring interventions effects**

Whether these interventions have actually yielded any significant results, remains unknown. Yet, it is possible to retrospectively see if and how these interventions affect the individual behaviour of users on online anonymous markets.

**Conclusions**

In conclusion, we can state that both the TOR-protocol and cryptocurrencies have potential disrupting effects in the illegal economy. The criminal justice approach to tackling crime in relation to online anonymous markets has still many challenges: both in science as in policing. That being said, although we see
that the level of the criminal innovation on these platforms is greater than in traditional crime, criminal activity on online anonymous markets is of incomparable proportions.

Internet technology is changing rapidly, and much of what we have written is therefore likely to change in the future.

Important websites

- Bitcoin blockchain explorer: https://blockchain.info
- Bitcoin wallet explorer: https://www.walletexplorer.com
- Dark web blogs: https://www.deepdotweb.com
- TNO Dark web solutions: https://dws.pm/
- TOR project: https://www.torproject.org/

References


