GDPO Global Drug Policy Observatory
reporting monitoring analysis

Swansea University
Prifysgol Abertawe

GDPO Situation Analysis

January 2015

Silk Road: After being closed twice, can the brand ever 'rise again?'

Alois Afilipoaie and Patrick Shortis

Since 2011 the Silk Road marketplace has been known as the flagship brand of Dark Net markets. For a long time it was the cornerstone of illicit trade over the Dark Net, despite being shut down by the FBI in October 2013 its successor Silk Road 2.0 was created in a month and quickly outgrew its predecessor. On November 6th 2014, the Silk Road 2.0 was closed in an international law enforcement operation dubbed 'Operation Onymous'[1]. Despite being taken down twice by law enforcement, the Silk Road was both a pathfinder and a trend-setter in the world of Dark Net markets. As a brand it will never be forgotten and may possibly continue to rise repeatedly as a hidden service on the Tor network, however as a marketplace the damage done by two busts may have finally put an end to its viability as a popular destination for those looking to engage in illicit trade.

The Silk Road marketplace (February 2011–October 2013)

Founded in February 2011, The Silk Road marketplace[2] created the most popular brand of any Dark Net market. Media attention in a 2011 article by Gawker writer Adrian Chen shot it to internet fame. Initially it sold a plethora of illicit items including drugs and weapons. Eventually it refined its identity as a market with libertarian philosophies and an ethical approach to its wares, it removed weapons from its listings as well as 'anything whose purpose is to harm or defraud', giving it an ethical edge over its competitors that many users enjoyed.

- The site was ran by an individual who called himself the Dread Pirate Roberts[3] (DPR) and a small group of support staff who handled disputes between customers, moderated forums and helped ensure that the websites security was up to scratch.

[1] See GDPO Situation Analysis *Operation Onymous: International law enforcement agencies target the Dark Net,* January 2015

[2] Named after the Silk Road, the historical trading route that connected Europe, the Middle East and China

[3] The name is based on a character from the 1987 film *The Princess Bride*. The hero is known as 'The Dread Pirate Roberts' who boasts a fearsome reputation for violence. It later transpires that this pseudonym has been handed down through generations of pirates to scare their victims into surrender without engaging in combat. This name has proved to be fitting as the Silk Road 2.0 was eventually led by an individual called the 'Dread Pirate Roberts 2'

- By the summer of 2012, a comprehensive measurement analysis of the Silk Road 1.0 showed that the marketplace generated revenues of about $143,000 per month for the market administrators, as well as total revenue for the vendors of $1.9 million per month. [4]

- There were over 22,000 individual items being sold on the Silk Road by a core of approximately 60 vendors, while most other vendors that created accounts on the Silk Road only stayed for 14 days at most.[5]

- By July 2013 the site had over 957,079 user accounts, although not all of them were buyers or vendors, with many being set up to either browse or monitor the site. The three countries with the most users were the US, UK and Australia.

The FBI were alerted to the sites existence in mid-2011 and began investigations, with other law enforcement agencies such as the Baltimore P.D. beginning their own at the end of 2011. Then at the beginning of 2012 a user named 'digitalink' was discovered to be 32-year old from Boston named Jacob Theodore George IV, he was arrested and provided intelligence on the markets operation.

In March 2012, a 29 year-old named Ross Ulbricht posted on a website named Stack Overflow to ask how to 'connect to a Tor hidden service using curl in php?'. He had used his real name in the post although later changed his the name to 'frosty' and changed the email address to frosty@frosty.com, an email address that law enforcement were able to tie to the encryption key of the Silk Road server at a later date. Ulbricht had also posted links on his social media to videos of Austrian economist Ludwig Von Mises. Dread Pirate Roberts had posted similar videos in the Silk Road forums.

On the 7th of January 2013 user and staff member Curtis Clark Green AKA 'chronicpain' was arrested in a sting operation set up by an undercover agent who had approached DPR with a large cocaine deal. DPR chose 'chronicpain' as the middle man for the deal, but once he was arrested he asked the undercover agent – who was still posing as a distributor - to execute Green. A hit was staged with Green's willing participation and DPR was sent photos of his apparently dead body as confirmation. DPR paid close to $40,000 to the undercover agent for the hit.

The FBI claimed to have found a misconfiguration with the login of the site that leaked the servers IP address. With the help of the Icelandic police, they were able to image the server and gather a wealth of intelligence.

Based on other arrests, as well as the 'frosty' post on Stack Overflow and some previous posts that could be traced back to Ulbricht's username on other forums, the FBI built a case against Ulbricht. By chance U.S. customs agents intercepted a package in which they found nine counterfeit identification documents with Ross Ulbricht's face on them. When questioned Ulbricht denied buying them but stated 'Hypothetically anyone could have purchased these on a website called Silk Road.' This admission gave them confirmation that he was aware of the site.

Ulbricht was arrested on October 2nd 2013 as he sat in a library in San Francisco. The FBI were careful to do the arrest whilst he was still using his computer so that they could prove he was the Dread Pirate Roberts, and apparently secured his computer whilst it was logged a section of the site reserved for staff.

At the same time the FBI seized the Silk Road Marketplace site and replaced its login screen with a seizure notice to alert its members. Users flooded to the only two reputable sites at the time to continue business, Blackmarket Reloaded (BMR) and Sheep Marketplace. BMR could not handle the sudden influx of traffic and closed shortly afterwards and Sheep Marketplace closed down after all of the Bitcoinss held on the site were stolen (many claim it was a scam set up by the sites moderator).

At the time of writing Ulbricht's trial is yet to begin and he continues to protest his innocence.

[4] See Christin, N. (2012) Traveling the SilkRoad: A Measurement Analysis of a Large Anonymous Online Marketplace. *Carnegie Mellon INI/CyLab*

[5] Ibid

Silk Road 2.0 (November 2013–November 2014)

The Silk Road 2.0 (SR2) was launched on November 6th 2013, just over a month after the first Silk Road was closed. This new site was crafted by members of the Silk Road forums, which were not seized by the FBI when the market was taken down. The new market launched with the same seizure notice left up by the FBI on it, but edited with a slogan stating ‘This hidden service has risen again’ written on it with the Silk Road logo attached.

- A new Dread Pirate Roberts was selected from the group that resurrected the new site, and was commonly referred to as DPR2. He took over the site with the clear intention to pass the moniker and leadership of the market over to someone else once it was up and running efficiently. After the arrest of several of the new sites moderators in December of 2013 DPR2 decided to leave and handed over control of the market to his second-in-command, a user called Defcon.

- The pace of Silk Road 2.0’s growth was unparalleled at the time: in a period of just over a month from its inception the narcotics listings grew from 500 to 3000[6]. By contrast, SR 2’s main rival, Black Market Reloaded needed nine months to grow from 2800 listings (Feb 2013) to 6600 (Dec 2013). Moreover, a significant proportion of BMR’s growth resulted from the seizure of the first Silk Road. By October 2014 SR2 was making sales of $8 million every month.

- Defcon claimed to have informants in the FBI and in January posted to the portion of the vendors-only portion of the site warning of a plan by the FBI to undertake a darknet-related drugs bust in Minnesota. He asked all members in those areas to ‘destroy information and go dark, or at bare minimum strengthen your operational security. Assume your house will be raided.’ Whether or not this was true is unclear

- An alleged hack in February 2014 saw all of the Bitcoins that were in the site’s escrow stolen and resulted in a loss of $2.4 million. It was argued that the former administrator of the marketplace, DPR2 was behind the hack, while Defcon claimed that an issue in Bitcoins, namely a ‘transaction malleability’[7] fault, caused the situation.

- In an unprecedented move, Defcon and his staff promised to pay back everyone who had lost Bitcoinss in the hack and claimed that they would forego their own staff wages to do so. They kept to their word, paying back up to 89% of the funds prior to the sites closure to all victims of the hack.

- The market suffered both from the hack, the doubt cast by the closure of the previous Silk Road and the arrest of SR2 moderators and the growth of new and very stable markets such as Agora and Evolution. Eventually it lost its place as the market leader to Agora. Improvements to the markets were often promised by staff but were either delayed or not delivered which frustrated many users enough to go looking into other markets.

- The market was hacked again in September 2014 and Bitcoins worth over 1.4 million were stolen. Rather than telling users and facing another loss of custom, Defcon took the site down temporarily and spoke to his support staff to discuss fixing the problem quickly so as to avoid another fiasco. He donated 1000 of his own personal Bitcoins in order to re-establish the site’s liquidity and within a month the site had made enough money to cover the loss.

On November 6th 2014 the site was seized once more, with law enforcement arresting computer programmer Blake Benthall and declaring him as the person behind the username Defcon. They also reported that he had admitted to everything after his arrest.

> ‘One of the primary targets was the Silk Road guy.’
>
> **Troels Oerting, Head of European Cybercrime Centre (EC3)**[8]

[6] See GDPO Situation Analysis from December 2013, *Silk Road and Bitcoins*

[7] The possibility for someone to use the Bitcoins network to alter transaction details to make it seem that a transfer of Bitcoins to a Bitcoins wallet did not occur when in fact it did occur

[8] Greenberg, Andy. (2014). Global Web Crackdown Arrests 17, Seizes Hundreds Of Dark Net Domains. [Available: http://www.wired.com/2014/11/operation-onymous-dark-web-arrests/. Last accessed 20/11/2014]

It transpired that the site had been one of the primary targets of Operation Onymous, a coordinated effort by law enforcement to shut down hidden services on the Tor network that we dealing in illicit goods and services. The operation saw 276 sites taken down overall including the SR2's competitor marketplaces Cloud 9 and Hydra.

The FBI also had an undercover agent from Homeland Security Investigations who had been part of the first Silk Road Marketplace and was invited into the inner circle of staff members at the very start of SR2, providing intelligence to law enforcement throughout the duration of the sites operation.[9]

It is still unknown how law enforcement undertook Operation Onymous, however it transpired that they had found the server for the site in Lithuania and imaged it in May 2014. The FBI claim Benthall had made an elementary mistake in registering a personal email address to the server for maintenance, which was blake@benthall.net.

When the FBI began building a case against him they found Bitcoins transactions in the hundreds of thousands of dollars that had been used to buy a luxury Tesla Model S car in January, with the dates and payments of Bitcoins corresponding to the time he started SR2.

Further to this they were able to use surveillance against him at his home to correspond the times that Defcon was online with the times that he was in his house. These facts in combination with subpoenas from Google of his login times to his email address and other investigative techniques gave them enough to make an arrest.

What Next - Silk Road 3.0?

- Whilst the first Silk Road Marketplace managed to meet customer expectations and deliver, SR2 despite being larger was marked by crises and instability, which devalued the brand as a whole.

> Unfortunately Silk Road is illegal, and one day this party will be over. Even if the software or the hardware never fail, people usually do. But know this – you cannot kill an idea. For this reason, there will always be a "silk road" just as there will always be an "anonymous". From here on in, it's a technology arms race.
>
> **Silk Road 1.0 user "The Business" - Silk Road Forums**

- After two separate busts by law enforcement where in both cases the Silk Road was the primary target, it seems ludicrous in the eyes of many Dark Net market users to have any part of a new Silk Road market as it is clearly a brand that law enforcement have singled out for investigation. This is despite the fact that SR2 was not as large as its competitor Agora by the time of the bust and did not sell weapons like Agora or Evolution (now the market leader) do.

- Hours after SR2 went down a small market known as Diabolus market quickly changed its name and logo to Silk Road 3.0. The market had a similar but markedly different appearance to the previous Silk Road sites, and was generally considered by many to be a scam. The response from Dark Net market users on reddit and darknet forums varied from cautious optimism to outright ridicule, with many believing that not only is the new site untrustworthy but that by using the Silk Road name they will inevitably be targeted by law enforcement.

- Whilst Silk Road as a brand was a market that won the respect and admiration of its users and competitors, and became an icon in the minds of many for its ability to undermine prohibition approaches to dealing with narcotics, it remains unlikely that we shall see a third viable market under the same name that gains a substantial market share of the overall trade that takes place on Dark Net markets.

[9] **U.S. Department of Justice. (2014).** *Criminal Complaint: Blake Benthall a/k/a "Defcon".* **http://www.justice.gov/usao/nys/pressreleases/November14/BlakeBenthallArrestPR/Benthall,%20Blake%20Complaint.pdf**

- It is clear from Operation Onymous that law enforcement worldwide have understood the threat of Dark Net markets and the way they have revolutionized illicit trade, and are now consistently undertaking operations to close these sites down. However, Dark Net markets – like real world drug dealers – are subject to the simple laws of supply and demand, and like conventional organized crime groups, cutting off the head of an organisation simply leads to a power vacuum for others to fill. It is clear that whilst the bust of the Silk Road 2.0 is another success for law enforcement agencies, it is one that will be short-lived as users flock to Agora and Evolution and the trade continues.

supported by

OPEN SOCIETY
FOUNDATIONS

About the Global Drug Policy Observatory

The Global Drug Policy Observatory aims to promote evidence and human rights based drug policy through the comprehensive and rigorous reporting, monitoring and analysis of policy developments at national and international levels. Acting as a platform from which to reach out to and engage with broad and diverse audiences, the initiative aims to help improve the sophistication and horizons of the current policy debate among the media and elite opinion formers as well as within law enforcement and policy making communities. The Observatory engages in a range of research activities that explore not only the dynamics and implications of existing and emerging policy issues, but also the processes behind policy shifts at various levels of governance.

Global Drug Policy Observatory

Research Institute for Arts and Humanities
Room 201 James Callaghan Building
Swansea University
Singleton Park, Swansea SA2 8PP
Tel: +44 (0)1792 604293
www.swansea.ac.uk/gdpo

@gdpo_swan

GdPo
Global Drug
Policy Observatory
reportingmonitoringanalysis