GDPO Global Drug Policy Observatory
reportingmonitoringanalysis

Swansea University
Prifysgol Abertawe

GDPO Situation Analysis

January 2015

Operation Onymous:

International law enforcement agencies target the Dark Net in November 2014

Alois Afilipoaie and Patrick Shortis

Subject

On the 6th of November 2014 the FBI and Europol working with other international law enforcement agencies declared that they had succeeded in a joint operation against several hidden services on the Tor Dark Net. The investigation, dubbed 'Operation Onymous' saw the successful closure of 267 '.onion' webpages making up 27 separate sites. Law enforcement agencies also made 17 arrests and seizures of $1 million in Bitcoin as well as assorted amounts of cash, drugs, weapons and computers.

Analysis

This is not the first high-profile Dark Net bust to have taken place, as previously the first Silk Road marketplace was busted last year in October 2013. However, in contrast to the last bust that was led by the FBI, Operation Onymous was an international operation with law enforcement agencies from the United States and Europe[1] working in partnership and declaring the operation as a cooperative effort.

The scale of the operation is incomparable to the last bust as this time multiple Dark Net sites were seized simultaneously, and where markets were seized law enforcement also targeted their forums so as to reduce the chance of members regrouping and rebuilding sites. This is clearly a lesson learnt from the bust of the first Silk Road, where the market was seized but the forum remained open, allowing members to develop a replacement market (Silk Road 2) within three months.

Among the sites seized was the Silk Road 2.0 whose leader 'Defcon' was reportedly arrested and unmasked as San Franciscan web developer Blake Benthall. Unlike Ross Ulbricht, who is alleged to be the administrator of the first Silk Road and still protests his innocence, law enforcement reported that Benthall admitted to being the site's administrator. It was also reported that there had been an undercover agent working from within the Silk Road 2.0's staff from its inception, which demonstrates law enforcements willingness to engage in long-term undercover operations on the Dark Net.

1 European law enforcement agencies involved were from Bulgaria, Czech Republic, Finland, France, Germany, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Netherlands, Romania, Spain, Sweden, Switzerland, and the United Kingdom

How was it done? : Tor's developers unsure

Tor's developers don't know how Operation Onymous was able to identify so many servers, but gave possibilities:

1. Poor operational security (opsec) on the part of administrators.
2. SQL injections – A type of attack that can be used to steal database information from a site.
3. Bitcoin deanonymisation – Research has shown that Bitcoin users could be deanonymised even when using Tor.
4. Attacks on the Tor network –Several possibilities listed for these types of direct attacks on Tor's infrastructure. [2]

Law enforcement agencies originally claimed to have seized 410 sites, which attracted attention from the Tor community as it suggested that vulnerabilities had been exploited in the browser's anonymising software. However, this figure was reduced to 267 sites seized at a later date, suggesting that the first figure was either quoted in error or was used as a disinformation tool to exaggerate law enforcement capabilities and deter users. Further investigation by security researcher Nik Cubrilovic has claimed that out of the 267 seized sites, 153 of them were either clone, phishing or scam sites that had been designed to steal login details. His research also shows that some sites that the FBI had declared to have seized were clones of the originals, with the real sites remaining live[3].

Based on his research Cubrilovic suggests that the operation was a 'broad, untargeted sweep' rather than a targeted attack on individual sites, and that rather than tracing site administrators, law enforcement went directly after companies hosting Dark Net sites, and then seized all of the sites on their servers.

How law enforcement managed to conduct the operation remains a topic of hot debate. The developers of Tor have admitted that they don't know how it happened and are asking for help from the wider research community. Already the Tor development team have received some insight from someone claiming to be the hacker 'Nacash' who developed and ran the hidden service Doxbin, however whether or not this has proved useful is as yet unclear.[4]

Law enforcement keep quiet on methods

'This is something we want to keep for ourselves… The way we do this, we can't share with the whole world, because we want to do it again and again and again.'

Troels Oerting, Head of the European Cybercrime Centre (EC3)[5]

The busts have seen users of Silk Road 2.0 flocking to alternative sites, in particular Evolution and Agora. Agora had been named in an October 2014 report by the Digital Citizens Alliance[6] as the biggest Dark Net market by product listings. However Evolution has now over taken it and is considered to be the market leader, with commentators putting this down to its sleek interface, quick loading times and security features

2 Biryukov, Alex. Khovatrovich, Dmitry. Pustogarov, Ivan. (2014).Deanonymisation *of Clients in Bitcoin P2P Network. [Available:* http://orbilu.uni.lu/bitstream/10993/18679/1/Ccsfp614s-biryukovATS.pdf

3 Cubrilovic, Nik. (2014). *Large Number of Tor Hidden Sites Seized by the FBI in Operation Onymous were Clone or Scam Sites.* Available: https://www.nikcub.com/posts/onymous-part1/. Last accessed 20/11/2014

4 torproject.org. (2014). *yes hello, internet supervillain here.* [Available: https://lists.torproject.org/pipermail/tor-dev/2014-November/007731.html. Last accessed 20/11/2014]

5 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]

6 Digital Citizens Alliance. (2014). *Busted but not Broken: The State of Silk Road and the Darknet Marketplaces.* Available: https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/5f8d4168-c36a-4f78-b048-f5d48b18dc0a.pdf. Last accessed 20/11/2014

such as multi-signature escrow. In terms of listings of products, Evolution had a growth of 26% in terms of its total listings whereas Agora experienced a decrease of 0.41% of its total listings, staying more or less on the same level. Andromeda, now placed third in the overall standings by total number of listings suffered a decrease of 21% of its total listings. The fact that none of these larger sites have been taken down by law enforcement when so many clone/phishing sites were seized would seem to support Cubrilovic's theory that hosting companies were targeted rather than individual sites.

Hours after Silk Road 2.0's closure, a new Silk Road site was up and running dubbed 'Silk Road 3.0'. However, this new iteration of the Silk Road moniker was actually a market known as 'Diabolous Market' that quickly capitalized on the opportunity the bust presented and changed its name and logo to attract users from the Silk Road 2.0. The response from Dark Net market users on reddit and darknet forums has 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.

Other markets also capitalized on the bust, Middle Earth Marketplace conducted an aggressive marketing campaign over a few forums where it advertised temporary suspension of their joining fee for vendors. As a result, they experienced a growth in the number of drug listings by 44%.

Whilst 17 arrests were made, there is a lack of clarity as to whether or not those arrested were administrators of sites or vendors within them. Either way it is clear that many sites administrators were able to avoid arrest despite having their sites seized. In the case of darknet market Cloud 9, its administrator allegedly took to reddit to claim that whilst they couldn't access the site, they still had all of their users Bitcoins and were working on creating a brand new market which they'd use to refund users and begin business again.

What Next?

- Operation Onymous demonstrates that law enforcement have made a renewed, sophisticated and cooperative effort to tackle illicit activity taking place over the Dark Net and have greatly improved their capabilities to do so. We can expect more arrests to follow as they continue to trawl through the wealth of information on vendors and customers that they will have garnered from copied servers and arrested administrators. This is what happened during the bust of the first Silk Road as it was followed by the arrest of several of its moderators further down the line.

> 'This is only the start of a wider campaign for the NCA to tackle the 'dark' or 'deep' web and the criminals exploiting it.'
>
> **Andy Archibald – Head of the National Crime Agency's (NCA) National Cyber Crime Unit (NCCU)** [7]

- Despite the likelihood of future arrests however, we can also expect the number of listings on Dark Net markets to recover and grow beyond pre-bust levels over the next year, as these markets continue to become more sophisticated, learn from their mistakes and gain popularity and users.

- Interestingly, law enforcement officials have even arrested and are pressing charges against owners of known scam sites. One Swiss man has been charged with running the site 'Black Market' that claimed to be able to sell weapons, drugs and forged currency amongst other products. The site had no escrow system and was generally considered to be a scam, however this has not deterred the Swiss authorities from pursuing prosecution against the suspect. Whilst this might be seen as good practice in deterring others from setting up Dark Net markets, this prosecution may also backfire for law enforcement. Scam sites are destabilizing to the Dark Net community and make many participants frustrated and distrusting of buying products online. By taking down so many scam and phishing sites, and discouraging others from setting them up by prosecuting those that run them, law enforcement may in fact increase real illicit trade over Dark Net markets by decreasing the uncertainty that scam sites provide to the markets.

7 The Guardian. (2014). *Silk Road: four suspected sellers of illegal drugs arrested in Britain.* http://www.theguardian.com/uk-news/2013/oct/08/silk-road-illegal-drugs-arrested-britain

- If Tor has been compromised (the worst-case scenario for administrators of darknet markets), it does not put an end to darknet markets. OpenBazaar is a decentralized market system that incorporates Tor but operates very differently to the centralized model used by Dark Net markets such as Evolution and Agora. In this model users have total control over their own storefront and are able to buy and sell whatever they want in a peer-to-peer system in which all members are equally-footed as the system's key components are self-regulated by nodes distributed throughout its users.[8] This would put an end to law enforcement's ability to shut a whole network down. Although OpenBazaar is currently in its testing phases we can assume that models like this will eventually become the dominant platform for illicit e-commerce in future.

- Similarly, issues with de-anonymising Bitcoin users over the Tor network will only lead to users taking to alternative cryptocurrencies such as Darkcoin, which is much more sophisticated in its anonymisation of its users and is increasingly being adopted by both markets and users.

- There is a possibility that this bust could result in blowback in the foreign policy goals for the US and its allies. The U.S. government continues to fund the Tor Project as Tor is used by human rights groups and activists in states with heavy internet censorship such as China and Iran. However, it is possible that the governments of these countries could learn the same methods used by law enforcement officials to seize Dark Net markets and use them to clamp down on dissidents in their own countries.

8 This is a similar model to Bitcoins or BitTorrent in which the network is distributed over a large number of users and cannot be taken down as there is no central server responsible for its operation

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

reporting monitoring analysis