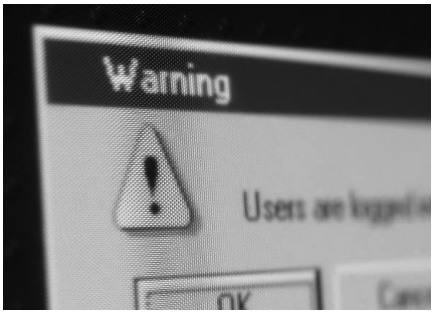
Inside Darknet: the takedown of Silk Road

Marie-Helen Maras reports on the unexplored underworld of cyberspace



The anonymity afforded by the Internet provides perpetrators with an environment within which they can operate with a low risk of detection. Nowhere is this more pronounced than in Darknet, which is considered the 'underworld' of cyberspace. Darknet consists of a collection of non-indexed domains; accordingly, these sites cannot be found using search engines like Google or Bing. To enter Darknet, Tor (the Onion Router), a privacy-enhancing application originally created by the USA Naval Research Laboratory, is used. Tor is 'an anonymous Internet communication system that provides individuals (and organisations) with the ability to share information and communicate over public networks without compromising their privacy' (Maras, 2014). When Tor is used, the 'user's Internet traffic is routed through a worldwide network of volunteer computers to conceal the user's location and Internet usage' (United States v Ross William Ulbricht, Superseding Indictment, 2013, 1).

There are legitimate uses for, and users of, Tor. Specifically, it has been and is being used 'by journalists, activists and campaigners in the USA and Europe as well as in China, Iran and Syria, to maintain the privacy of their communications and avoid reprisals from [their respective] government[s]' (Ball et al., 2013). This article examines the illicit use of Tor and Darknet: looking in particular at Silk Road. Following this, it explores the investigation of Silk Road and the implications of the arrest of the site's administrator.

Darknet has been used to buy and sell drugs, weapons, counterfeit documents (e.g. passports, driver's licenses, social security cards, and utility bills, to name a few) and counterfeit money, as well as to provide a medium for contract killers to solicit clients. It has also been used to buy and sell credit card information (complete with a user's name, address, phone number, card verification value, and expiration date), child pornography, pirated software and other copyrighted materials, malicious software (or malware), and computer hacking services and tools (to gain unauthorised access to accounts and systems). For example, a vendor on a site in Darknet offered 'to hack into Facebook, Twitter, and other social networking accounts of the customer's choosing, so that…[a user can read, write, delete, upload, and view all of the personal information of a user or users]; another listing offered tutorials on "22 different methods" for hacking ATM machines' (*United States v Ross William Ulbricht*, Criminal Complaint, 2013, 10).

Silk Road: a Darknet site

A high profile case that brought worldwide attention to Darknet was the taking down of Silk Road by the Federal Bureau of Investigation (FBI). Silk Road, a black market site in Darknet, offered a variety of controlled substances for sale and purchase, including (but not limited to): heroin, cocaine, amphetamines, ecstasy, and cannabis. Silk Road enabled individuals to buy drugs anonymously anywhere in the world, as long as these individuals were using anonymising software and knew the exact address of the site. This site also enabled users anywhere in the world to buy and sell false identifications and other forms of contraband (ibid). The currency used for this, and other similar sites (e.g. BlackMarket Reloaded), are Bitcoins.

Cryptocurrencies, such as Bitcoin, Namecoin, Litecoin, Peercoin, and Ripple, are peer-to-peer commodities. With cryptocurrencies, no third-party involvement exists in money exchange; the money is simply moved between players' accounts. Bitcoins are virtually mined using computers to solve complex algorithms. There are a finite number of Bitcoins.

Complex algorithm

Accordingly, to prevent the timing out of the supply of Bitcoins, after a complex algorithm is solved and a batch of new Bitcoins is 'virtually unearthed,' the algorithm to be solved for the next batch of Bitcoins becomes more complex. This digital currency (and others like it) further enables anonymous illicit transactions because it is an unregulated form of currency and can be cashed out outside of regulated banking systems.

To conduct transactions on Silk Road, buyers and sellers had to have at least one Bitcoin address associated with an account on the site. Bitcoins are purchased from a Bitcoin exchanger and sent to the Bitcoin address associated with the Silk Road account. If a buyer makes a purchase on Silk Road, the Bitcoins are transferred to an escrow account on Silk Road. When the transaction is completed, the Bitcoins are transferred from the Silk Road escrow account to the Bitcoin address associated with the Silk Road account of the seller. To protect the anonymity of these transactions, Silk Road uses a 'tumbler' which sends 'all payments through a complex, semi-random series of dummy

10.1080/09627251.2014.984541

transactions…making it nearly impossible to link…[a] payment with any coins leaving the site' (*United States v Ross William Ulbricht*, Criminal Complaint, 2013, 14).

The end of Silk Road

The administrator of Silk Road, Ross William Ulbricht (aka Dread Pirate Roberts), was arrested in October 2013. As the administrator, Ulbricht was responsible for the: management of administration staff; control of Silk Road server infrastructure; control of Silk Road policies; and control over the proceeds of Silk Road sales (United States v Ross William Ulbricht, Criminal Complaint, 2013, 16-21). Essentially, he controlled all aspects of Silk Road and provided a platform to users for the buying and selling of illicit substances, goods, and services, for which he received commissions in the tens of millions of dollars (*United States v Ross William Ulbricht*, Superseding Indictment, 2013; *United States v Ross William Ulbricht*, Indictment, 2013, 2 and 6).

In Baltimore, Maryland, Ulbricht was charged with 'knowingly and unlawfully combined, conspired, confederated and agreed with others…to distribute and possess with intent to distribute controlled substances' and attempted murder of a former employee (*United States v Ross William Ulbricht*, Superseding Indictment, 3 and 10). Ulbricht was also charged in New York with conspiracy 'to violate the narcotics laws of the United States,' by, for example, distributing and possessing 'with the intent to distribute controlled substances' and the delivering, distributing, and dispensing of 'controlled substances by means of the Internet' (*United States v Ross William Ulbricht*, Indictment, 2014, 2).

Ulbricht was also charged in New York with: money laundering conspiracy; computer hacking conspiracy; conspiracy to murder a witness; and continuing criminal enterprise (*United States v Ross William Ulbricht*, Criminal Complaint, 2013; *United States v Ross William Ulbricht*, 2014). With respect to the latter charge, Ulbricht engaged in a continuing criminal enterprise 'in concert with at least five other persons with respect to whom Ulbricht occupied a position of organiser, a supervisory position, and a position of management, and from which such continuing series of violations Ulbricht obtained substantial income and resources' (*United States v Ross William Ulbricht*, Indictment, 2014, 5-6). Ulbricht was charged under the *Continuing Criminal Enterprise Statute of 1970* (otherwise known as the Kingpin Statute), a law commonly used to target the heads of large-scale drug trafficking operations. To protect his criminal enterprise, Ulbricht even solicited murder-for-hire for those he believed posed a threat to him (ibid).

The aftermath: conclusions and recommendations

This Silk Road investigation provided a wealth of data on the inner-workings of the site and transactions occurring through the site. Additionally, it provided information on how buyers and sellers were concealing illicit activity. For instance, the Wikipedia entry for Silk Road contained both a Buyer's Guide and a Seller's Guide containing information on how to avoid detection by authorities (*United States v Ross William Ulbricht*, Criminal Complaint, 2013, 11). The Buyer's Guide instructed potential buyers of items on Silk Road to have the items sent to a different address from their own and to subsequently 'transport [the item] discreetly to its final destination' (ibid). The Seller's Guide instructed sellers on Silk Road on how to avoid detection by electronic sniffers or dogs by vacuum sealing packages containing drugs (ibid).

When the administrator of Silk Road was arrested, many sites like Silk Road existed in Darknet, each offering similar illicit substances, goods and services. Furthermore, after Silk Road was shut down, it was soon replaced by Silk Road 2.0, where the illicit purchasing of controlled substances, goods, and services continued. The administrators of Silk Road 2.0 were also subsequently arrested. Despite the recent arrests, the privacy enhancing technologies used and the anonymity afforded to users of Darknet has made the targeting of lawbreakers in this forum particularly challenging for authorities. The same holds true for terrorists seeking to use this forum. Darknet sites have been used by terrorists to communicate undetected, distribute propaganda, obtain supplies for operations, and raise funds for malicious activity. Apart from anecdotal evidence, (Hutson and Miller, 2010), the nature and extent of these occurrences remains largely unknown. In fact, little is known about Darknet and its potential uses; research in this area is also largely absent. What's more, the number of Darknet sites and individuals using these sites is unknown. Research concerning Darknet is required to fill this gap in available research and provide much needed information on black market operations in the predominately unexplored underworld of cyberspace. ■

Dr Marie-Helen Maras is Associate Professor, John Jay College of Criminal Justice, City University of New York

References

Ball, J., Schneier, B. and Greenwald, G. (2013), 'NSA and GCHQ target Tor network that protects anonymity of web users', *The Guardian*, 14 October.

Hutson, B. and Miller, M. (2010), *Beware the Darknet*, Durham: Procysive Corporation, http://bit.ly/1nvwGd5

Maras, M-H. (2014), *Computer Forensics: Cybercriminals, Laws and Evidence*, 2nd edition, Burlington, MA: Jones and Bartlett, p.297.

United States v Ross William Ulbricht, Criminal Complaint, Sworn Statement of FBI agent Christopher Tarbell, (NY, Southern District Court of NY, 2013).

United States v Ross William Ulbricht, Indictment, No 14 CR 068 (NY, Southern District Court of NY, 2014).

United States v Ross William Ulbricht, Superseding Indictment, No CCB-13-0222, slip op (MD, District Court in Baltimore County, MD, 2013).