Silk Road bust unmasks our misconceptions on anonymity

October 9 2013, by Catherine Flick

You're going to have to try a bit harder if you want to be really anonymous. Credit: moirabot

The US National Security Agency and the UK's GCHQ have upped the stakes in the battle for internet privacy by targeting users of Tor.

Not only have the NSA documents leaked by Edward Snowden up until

this point given us a window into secretive US and UK government activities but they have raised some serious concerns for everyday internet users. Widespread surveillance of internet and phone use, including email, video, and voice-over-IP systems has led to a remarkable increase in the number people turning to the open-source Tor Project, an anonymising network service that has been used to enable private internet use for over a decade.

How Tor works

Tor is most popularly used through its packaged Tor Browser Bundle, which runs a customised version of Mozilla Firefox along with its own software that sets up the Tor connections for the user. Users are then able to reasonably easily anonymise their internet use – though there are some drawbacks, including slow speeds.

Tor works by bouncing a connection through several routers in the network, obfuscating the origin of the connection along the way. The net result is that the end server doesn't know where a request is coming from and the message is encrypted until it leaves the Tor network. Theoretically, that means that adversaries are not able to monitor the connection. The user is technically anonymised by the software, with only a minimal amount of information (the fact the user is using the Tor Browser) "leaked" along the way for snoopers to pick up.

Within the Tor network alternatives to public internet services exist. These "hidden services" include email, forums and chat channels and can be used without requiring the user to reveal any information about themselves. The flip side of the hidden services capability of Tor is that it can allow for some less than savoury activities to be carried out anonymously. One such example was the Silk Road – a forum which was used to buy and sell drugs.

Silk Road has been called the worst-kept secret in hidden services. It's probably not surprising, then, that worldwide law enforcement were interested in, at the very least, breaking it up, if not also arresting those responsible for aiding drug sales. And last week, that's precisely what happened.

Two types of anonymity

Alleged founder Ross Ulbricht was arrested and charged with carrying out various conspiracies under the Princess Bride-inspired pseudonym The Dread Pirate Roberts. The charges levelled against him range from narcotics trafficking, computer hacking and money laundering to soliciting murder. It is probably no surprise, either, that the FBI has also gained access to the content of the Silk Road database, including mailing addresses and other potentially identifying information about those involved in the system.

How the FBI located the Silk Road servers is still uncertain. But what has become clear is that Ulbricht had become complacent about his identity anonymity – the very type of anonymity that Tor does not protect. Even the most secure anonymising service cannot prevent a user saying precisely who they are through it. And you don't even have to be this obvious – profiles can be built of users who leak out tiny pieces of information about themselves over a long period of time, or correlated with public internet use. Ulbricht, for example, posted to public internet websites using an email address linked to his real name. Another user has been charged after apparently being traced through return addresses when posting drugs.

The important message in all of these revelations is that all the technical wizardry in the world can't save you from yourself. The Silk Road bust and subsequent arrests; the taking down of various other hidden services through a major malware attack perpetrated by the FBI that occurred last

month taking with it Freedom Hosting and its child abuse image sites: it all shows that despite the superior technical anonymity provided by the Tor Project (zero-day vulnerabilities aside), nothing technical can prevent complacent users from giving their own information away.

If you want to remain truly anonymous, you must constantly assume that someone is watching exactly what (and when) you're writing, and take appropriate measures. As we saw with Lavabit, governments have the ability to pressure companies to provide them with "back doors" into their otherwise secure environments. This is where identity anonymity comes in. It is not enough to simply use a secure service – you have to assume that the information you send through it may eventually be traced through some means back to oneself.

This scenario has implications not just for those small minorities of users wishing to trade drugs or child abuse images, but has huge implications for whistleblowers like Edward Snowden (who used Lavabit), journalists, people in oppressed countries wishing to speak out or organise against their governments, and many other legitimate uses of such technologies – and even for those who just wish to carry out everyday activities with proper privacy from snooping government agencies.

The increase in use of Tor after the NSA revelations shows that these everyday users are on the rise – it's important for them to be educated in both technical and identity anonymity so they know the risks. Perhaps this is impossible though – humans are naturally social creatures who enjoy sharing information about themselves to feel part of a community. Our very nature makes being truly anonymous a monumental task.

Source: The Conversation