Can you really be identified on Tor or is that just what the cops want you to believe?

July 28 2014, by Eerke Boiten, Julio Hernandez-Castro

Credit: Ylanite Koppens from Pexels

Have the UK police successfully broken anonymity on the internet? They certainly seemed to imply as much when the National Crime Agency proudly announced last week that it had made 660 arrests after an operation to identify people viewing indecent images of children

online.

The announcement raises questions about just how anonymous it is possible to be online, particularly in the dark net and through systems like Tor, which is used by criminals, but also many others with legitimate reasons for wanting to remain anonymous such as journalists, whistleblowers, and political activists under repressive regimes.

We should also treat the NCA bust with some scepticism, given its very convenient political timing.

Operation Notarise

When the National Crime Agency made its big announcement about Operation Notarise, it was obviously good news. Hundreds of people suspected of crimes could soon be under lock and key thanks to its efforts. The agency also said that it would not reveal how it identified the suspects so that it could use the same method to track them down in the future. There was a clear message sent out to wrongdoers in the official press release, though: "We want those offenders to know that the internet is not a safe anonymous space for accessing indecent images, that they leave a digital footprint, and that law enforcement will find it".

It made a similar statement after arresting four people suspected of being involved in drug selling through now-defunct dark web marketplace Silk Road, warning that even the most tech-savvy criminals make mistakes and leave traces.

The NCA is clearly saying that it can find you, even if you are using the dark net. And in the context of child porn, it would be reassuring if it were right. But it may also be the case that the security software currently available is so difficult to use that, in practice, anyone will indeed make mistakes. Others would say that the NCA has picked up

only low-hanging fruit in its 660 arrests, identifying the dumb ones – the people who use anonymity tools inexpertly or maybe not at all.

Breaking Tor

In its infamous Tor Stinks document from June 2012, the NSA revealed that it does not believe in blanket attacks on Tor – even gathering and retaining all potential Tor traffic all the time would just not work.

But targeted attacks, including in the imaginatively titled EPICFAIL programme, which seeks to capitalise on inexpert use of Tor to identify people, might be more successful. There are NSA and GCHQ programmes that look for cookies that survive Tor sessions (with the standard Tor browser bundle there shouldn't be any). The most powerful attacks against Tor use the NSA QUANTUM programme. This, among other things, employs very fast servers in central locations on the internet backbone to intercept and replace "suspicious" internet communications.

Other attacks against Tor have been known for a long time. Researchers showed in 2005, for example, that internet traffic analysis could be used to link different Tor connections, though this could not be used to directly identify the users involved.

… for less than $3K?

There was a flurry of internet excitement recently when researchers from Carnegie Mellon University revealed they would make a presentation at the 2014 Black Hat conference that showed you don't have to be the NSA to break Tor. In fact, they would reveal, a large number of Tor users could be identified within a few months and on a budget of less than $3,000. Interestingly, Carnegie Mellon had the talk cancelled for legal reasons and the Tor development team are fixing the

bug they identified.

The story is unlikely to end here. It seems that the current state of play is that limited targeted attacks are possible, but blanket attacks are not. This could, of course, change with new developments as a lot of research is going on trying to devise new attacks against Tor.

Surveillance, and timing

The debate about whether Tor can be truly anonymous will rage on but it's the timing of the NCA announcement that is perhaps most notable. Arrests had been made under Operation Notarise from at least April onwards but it chose not to say anything until July.

The announcement finally came on July 16, the very day the UK parliament was to vote through the Data Retention and Investigatory Powers bill ("DRIP") as emergency legislation. The public argument for the need for this bill was that "communications data of this kind are used in 95% of serious and organised crime investigations, counter terrorism investigations and online child abuse investigations".

The 95% figure seems to be based on communications data being used in serious and organised crime investigations by the Crown Prosecution Service. What is not clear is which fraction actually referred to data resulting from targeted rather than blanket surveillance, and in how many cases retention had played a role.

Any successful attack against Tor anonymity would probably have been based on targeted surveillance and perhaps even on direct interference. This strongly suggests that the conveniently timed NCA success actually lends little evidence to support the need for blanket data retention powers as included in DRIP.

All in all, it seems that this operation, with its very positive impact of putting hundreds of very dumb and dangerous criminals behind bars, has some shadows. Its convenient political timing should make us regard the whole thing with scepticism. Particularly when, like in this case, the authorities seem not to have used any new or powerful technology but mostly achieved an easy, timely and effortless media victory. On the other hand, it is probably not realistic to aim for much more with the modest resources that our law enforcement has at its disposal.

Source: The Conversation