How a cyber attack hampered Hong Kong protesters

June 14 2019, by Stanley Shanapinda

Credit: CC0 Public Domain

Massive public protests taking place in Hong Kong over the past week are aimed at a new extradition law, known as the Fugitive Offenders Ordinance, that would see accused criminals extradited to mainland

China to face prosecution.

Hongkongers feel the law could be used to legalise the kidnapping of people who express views, and act in ways, that are not popular with the Chinese government. The same law could also be used to extradite tourists and visitors to China who are arrested on suspicion of having committed these crimes.

Protesters want the bill scrapped. For now, debate of the legislation has been postponed.

Organisers say one million people turned out for the protests, while police estimate the number was around 240,000. Either way, it was a significant number of Hong Kong's 7.5 million population. Commentators on Twitter remarked on how well organised the protesters were.

So, how did they do it?

Protesters across the world are using new technologies to organise. Social media platforms were used to share information about the Hong Kong protests. And messaging apps, such as Telegram and WhatsApp, were essential for coordinating with other protesters.

Telegram as a protest tool

In choosing a messaging app, organisers are looking to communicate effectively while avoiding surveillance. Telegram, which launched in 2013, has become a more secure competitor to WhatsApp.

Telegram says it has standard end-to-end encryption for its chats, to prevent spying on the contents of communications.

There is the "cloud chats" option for group messaging. Telegram also allows for "secret chats" between two people. These chats are stored on the phones rather than in the cloud, and can be set to self-destruct at a time determined by the user.

Unlike WhatsApp, Telegram hasn't suffered major hacks in the recent past. Earlier this year, WhatsApp was reportedly infected with the Pegasus spyware as part of an attempt to access the messages of a UK-based human rights lawyer who was working on a case for civil rights activists. During the 2014 protests, WhatsApp was also reportedly attacked to spy on Hongkongers.

Telegram is a partially open source platform. Anyone can contribute to strengthening its security by looking for and fixing vulnerabilities, which can help to prevent hacks like those from Pegasus.

Telegram therefore offered Hongkongers a messaging service they could use with a bit more confidence, or so the organisers thought. But the use of spyware isn't the only method available to those who might want to disrupt the communications of protesters.

Telegram becomes a target

The administrator of a 30,000-member Telegram chat group, which was used to organise the protests, was arrested on Tuesday. Ivan Ip, 22, was accused of conspiring to commit a public nuisance. Ip told the New York Times:

"I never thought that just speaking on the internet, just sharing information, could be regarded as a speech crime […] I'm scared that they will show up again and arrest me again. This feeling of terror has been planted in my heart."

In a further show of force, Telegram was also targeted in a distributed denial-of-service (DDoS) attack during the protests.

DDoS attacks use botnets, which are computers that have been compromised by malicious software and then used to launch cyber attacks in an automated fashion. The owner of the computer may not even know that their property was used as a tool to suppress civil rights activists.

Telegram's servers were flooded with junk communications at rate of 200-400 gigabits per second, slowing functioning of the service until it was ineffective or unusable.

Based on past trends, this size of an attack is likely to have been carried out by a state actor. Telegram founder and CEO Pavel Durov said source IP addresses indicated the geographic location of the attacks were mainly originating in China.

This disruption appears to have been coordinated to occur at the height of the protests for maximum impact, creating a chilling effect on the ability of protesters to organise and communicate.

The effect of the attack was global, impacting Telegram users in other countries like the United States. This shows how targeted internet censorship techniques in one country could punish citizens of another.

Forcing protesters into a corner

By making Telegram unusable, the cyber attack redirects the communications of organisers onto less secure platforms, where vulnerabilities can be exploited.

Communications on these platforms might be more easily intercepted,

and metadata and location information might be available from telecommunications companies and ISPs. This can heighten protesters' fears of being identified and prosecuted for their political actions.

The power of governments to attack and disrupt the communications of protesting citizens has a chilling effect on the universal right to march and to protest. Social media hacking tools, which are sold to repressive governments to spy on their own citizens, further erode the right to free speech and to organise political activity.

In this environment, demand for secure social media apps will only increase out of a basic necessity to break free from surveillance, and for protection against authoritative regimes around the world.

Provided by The Conversation