This article was first published in the May 2020 issue of the Thought Leaders 4 FIRE Magazine. Permission given for republishing on SLW.

CIVIL REMEDIES FOR IDENTIFYING AND INJUNCTING HACKERS IN SINGAPORE

Authored by: Danny Quah – Providence Law Asia (Singapore)

On 9 May 2020, Bleepingcomputer.com published an article with an ominous sounding title ***"Hacker group floods dark web with data stolen from 11 companies"***. In the article, it was revealed that a hacking group known as Shiny Hunters had hacked into the databases of companies such as Tokopedia (Indonesia's largest online store) and Unacademy (one of India's largest online learning platforms), and had begun selling the user databases over the Dark Web for between $500 to $5,000 each.

Can the victims of the hack take any civil action in Singapore against the hackers to identify and injunct them? While there have not been any published decisions in Singapore on this, this author seeks to draw lessons from two recent English decisions on this issue.

1 AA v Persons Unknown who demanded Bitcoin on 10th and 11th October 2019 and others [2019] EWHC 3556 (Comm) ("AA")

In *AA*, a company's computer systems were hacked and encrypted by hackers (i.e. the 1st Defendant) who demanded a ransom to decrypt the said systems.

The company's insurers paid the ransom in Bitcoin, and subsequently commissioned an investigation to track the movement of the Bictoin. The investigations revealed that a substantial proportion of the Bitcoin was transferred to a specified IP address (i.e. the 2nd Defendant), which was linked to an exchange known as Bitfinex operated by the 3rd and 4th Defendants.

The insurers applied to the English Court seeking, inter alia, a Bankers Trust / Norwich Pharmacal order requiring the 3rd and 4th Defendants to provide certain information in relation to a crypto currency account owned or controlled by the 2nd Defendant and a proprietary injunction in respect of the Bitcoin held in the account of the 4th Defendant, with consequential orders to serve the orders outside of the jurisdiction in the British Virgin Islands.

After determining that Bitcoin was a form of property capable of being the subject of a proprietary injunction, Mr Justice Bryan granted the proprietary injunction against the defendants. He held that the 1st and 2nd Defendants were the persons who in fact committed the extortion and were paid the ransom, while the 3rd and 4th Defendants were holding Bitcoin belonging to the applicant which had come into their possession in the furtherance of a fraud.

Mr Justice Bryan further agreed that an order for service out of jurisdiction should be made on the basis that the claim was being made to prevent the defendants from doing an act within the jurisdiction, and there was a claim by the applicant in tort where damage was suffered within the jurisdiction as the insurer is an English insurance company and had paid the Bitcoin from monies taken from an English bank account. For practical purposes, Mr Justice Bryan also agreed that alternate service on the 1st and 2nd Defendants could be effected via the email which demanded the ransom. Similarly for the 3rd and 4th Defendants, service could be effected via the emails which they used to correspond with the applicant.

As for the Bankers Trust / Norwich Pharmacal order, Mr Justice Bryan held that the 3rd and 4th Defendants ought to provide the identify, address and any associated information of the 1st and 2nd Defendants that they may possess. Mr Justice Bryan also made a self-identification order against the 1st and 2nd Defendants as he considered the information necessary to police the proprietary injunction that he had granted.

2 PML v Person(s) unknown (responsible for demanding money from the Claimant on 27 February 2018) [2018] EWHC 838 (QB) ("PML")

In *PML*, the applicant's computers were hacked and a large quantity of data was stolen. The defendant subsequently sent an email to the directors of the applicant seeking a ransom of £300,000 worth of Bitcoin in exchange for not publishing the data online. In the midst of negotiating with the defendant, the applicant applied to court, without notice to the defendant, for an interim non-disclosure order to restrain the threatened breach of confidence and for delivery-up and/or destruction of the stolen data.

The interim injunction was granted by Mr Justice Bryan at first instance, and the order was served on the defendant via the email address used to communicate with the applicant. Following the applicants' own investigations, the applicant identified a number of websites which hosted the stolen documents, and served the injunction order on them. This resulted in the hosting companies blocking access to the documents or deleting them following service of the injunction order.

On the return date, Mr Justice Nicklin continued the injunction order and further granted an order against the Defendant to identify himself and provide an address for service. Mr Justice Nicklin noted that the Defendant may be overseas, and granted permission to the applicant to serve the claim form out of jurisdiction on the basis that the claim was for breach of confidence and the detriment would be suffered within the jurisdiction were the threatened publication take place.

3 Lessons for Singapore

While the persons unknown injunction and self-identification orders have yet to be deployed in Singapore in the manner utilised in AA and PML, this author is of the view that the Singapore courts will be likely to make similar orders in the appropriate case.

First, the Singapore International Commercial Court has not had any difficulty regarding cryptocurrency as a property in the general sense as seen in the case of *B2C2 Ltd v Quoine Pte Ltd* [2019] 4 SLR 17. Hence, a proprietary injunction can latch onto cryptocurrency.

Second, an applicant may take the position that an action should not be defeated even if there was no identified defendant at the start of the action, as long as there are actual defendants identified and property joined to the action by the time of the trial. The applicant can point to the High Court's general power in para 5(a) of the First Schedule of the Supreme Court of Judicature Act to grant interim interims in support of legal proceedings at any time, without any express requirement that an actual defendant be invoked before the power can be invoked. Hence, the

Third, pre-action discovery and pre-action interrogatories (i.e. the Singapore equivalent of Bankers Trust / Norwich Pharmacal orders) are expressly permitted under Singapore's Rules of Court. These applications can be deployed to require a party to self-identify or to require a cryptocurrency platform / exchange to identify the individual(s) behind an IP address.

Fourth, alternative or substituted service via social media (e.g. Skype / facebook / internet message board) or email can be granted by the Singapore courts. This was done in *Storey, David Ian Andrew v Planet Arkadia Pte Ltd* [2016] SCHCR 7.

In conclusion, an applicant who has experienced a digital hack will likely be able to avail itself of certain civil remedies under Singapore law to seek relief from the consequences of the hack.