JAPAN

Japan Supreme Court acquits defendant in Coinhive case

Abe & Partners

Takanori Abe

A recent case concerning computer mining was among the 10 most complex in Japan, according to the Ministry of Justice. Takanori Abe of Abe & Partners analyses the Supreme Court's decision.

Summary of the case

This complex case concerning computer mining involves a party known as Y that was operating a music website (referred to as X) in September 2017.

Coinhive is a web service launched by the Coinhive team in September 2017. The service provided the operators of a website who subscribed to the service (the subscriber) with the program code enabling the subscriber to obtain the program code (the main program) to execute a mining operation.

This operation enables the subscriber to instruct the central processing units (CPUs) used by website visitors to calculate an approval of recording transaction histories to the transaction ledger of the cryptocurrency Monero, without the visitor's consent.

The operation enables the subscriber to acquire the cryptocurrency as a reward upon the success of the calculations: 70% of the cryptocurrency was assigned to the subscriber and 30% to the Coinhive team. When the program code was installed on the subscriber's website, the mining would be executed by the visitor's computer and the subscriber could receive a share of the reward.

The mechanism of mining used by Coinhive was as follows:

1. A visitor browses the website on which the above-mentioned program code is installed.
2. On receiving certain commands of the program code, the visitor's computer is automatically connected to the server computer to which the main program is installed.
3. The main program is loaded and receives a command for mining.
4. The CPU conducts a calculation subject to the above command.
5. The mining process ends when the visitor ceases browsing.

Y subscribed to Coinhive in order to earn profit via its website X on September 21 2017 and was provided with a program code. Y then installed the program code with the explanation of the site key assigned to him (the program code) to X on the server computer and stored it in the file constituting X during the period of dispute.

Although the mechanism to have a visitor's computer conduct mining to earn profit from a website was not known to general users at that time, Y kept storing the program code without either installing specifications to obtain consent from visitors, or providing an explanation regarding the mining or representing the fact that mining was processing.

Y adjusted the CPU usage of the visitor's computer to 0.5. As a result, the power consumption of the visitor's computer increased slightly and the processing speed of the CPU slowed down somewhat. Those effects were not large enough to be recognised by visitors and there was no significant difference compared to programs displaying advertising that are widely used on websites.

Judgment of January 21 2022, Supreme Court

The Yokohama District Court acquitted Y. The Tokyo High Court found Y guilty and imposed a fine of Y100,000 ($900). The Supreme Court (Presiding Judge Yamaguchi) reversed the judgment and rendered a further judgment finding Y not guilty.

The crime of making of electronic or magnetic records containing unauthorised commands is intended to protect the social trust that programs for data-processing by computers do not give "unauthorised commands to prevent a computer from performing functions in line with the user's intention or have it perform functions against the user's intention".

Consequently, this crime protects the social functions of computers, given that malicious programs executed against the user's intention cause damage to society and constitute a serious problem. To achieve this purpose, the crime punishes, under certain conditions, the creation, provision, storage, etc of programs that give commands that are against the user's intention, socially unacceptable and unauthorised.

It is reasonable to consider that "against the user's intention" means when the actual operation of the program differs from the operation which general users can recognise. In confirming the operation that general users are to recognise, not only the content of the program operation but the name of the program, the content of the explanation of the program operation and the assumed way of utilising the program need to be considered.

In addition, it is reasonable to consider that lack of authorisation refers to a socially unacceptable program from the perspective of protecting the social trust in data-processing by computers and the social functions of computers. In addition to the content of the operation of a program, it is important to consider whether or not and to what extent the operation of the program has an impact on the functions of computers and data-

processing by computers and how the program is supposed to be used.

The website X was not designed to obtain consent for mining to be executed while browsing, and there was no explanation regarding mining and no representation that mining was executed. The mechanism of having the visitor's computer execute mining as a method to earn profit from website was not generally recognised.

Taking these circumstances into account, it could not be said that general users should recognise the operation of the program code. Thus, "against the user's intention" is affirmed.

The impact on the functions of computers and data-processing by computers which are important factors in light of the legal interest is limited to using the CPU of the visitors' computers while they are browsing website X. The effect is the slight increase of power consumption and slowing down the processing speed of the CPU and is not large enough to be recognised by visitors.

In addition, the mechanism that an operator of a website earns profit through browsing is important for information distribution through the website. Y used the program code with such a profit-making mechanism. There is no significant difference regarding the impact on the functions of visitors' computers and information processing by computers between the program code and the socially accepted advertising programs.

These programs are executed without visitors' prior consent and use a visitor's computer to a certain degree while browsing in a similar way. Both programs can be considered socially acceptable.

Furthermore, the mining itself, which is the content of the operation of program code, is a mechanism to ensure the reliability of cryptocurrencies. It is therefore difficult to consider it to be socially unacceptable.

As a consequence, the program code cannot be considered as socially unacceptable and lack of authorisation cannot be affirmed.

Practical tips

This case was selected by the Ministry of Justice as one of 10 complex and difficult cases, and has caused intense controversy. Evaluations of the case have been divided even among internet users.

Some users said that Y was making money by using the CPUs of other users' personal computers without consent and this was ethically unacceptable; while other users argued that the program is not a computer virus, is no different from online advertising and can be regarded as suggesting an alternative means of monetisation to online advertising.

There were also opinions that if this program is deemed illegal, the owner of any kind of website would be required to announce to every visitor that it would use the CPU of visitors' computers.

The police argued that Y was forcing visitors to the website to execute mining operations without letting them recognise it and it is malicious as it was using other people's computers to earn money without any notice.

The prosecutors argued that it is salami-slicing and the effect is not minor, and is equivalent to cryptojacking and is policed as cybercrime internationally. The prosecutors also argued that if the activity were not found to be illegal, Japan would become the target of abusive use of CPUs from all over the world without consent.

However, the defence counsel argued that there is no practice of obtaining the consent of the visitor in executing individual JavaScript programs; that if such programs were illegal, it is difficult to draw clear lines between this case and Google Analytics or other advertisements; that it would give a chilling effect on program development in Japan; and that in this case, JavaScript was installed on the website of Y making it completely different from cryptojacking.

There was a view pointing out that when the bill for this crime was passed by the Committee on Judicial Affairs, House of Councillors, there was a supplementary resolution stating: "In investigating this crime, efforts should be made to utilise it appropriately so that it will not have any negative impact on the development and distribution of software, taking into account the freedom of expression guaranteed by the Constitution of Japan."

Another view pointed out that the program is excluded from the type of computer virus that was assumed at the time of legislation. Norton blocked access to sites with Coinhives embedded.

After the judgment of guilt in the Tokyo High Court, the defence counsel sought opinions on the website of the Japan Hackers Association, and submitted 47 written opinions to the Supreme Court.

The Supreme Court affirmed the "against the user's intention" finding, pointing out that there was no consent from the visitor, no explanation or representation of the mining, and no general recognition of the mining. However, the Supreme Court did not find lack of authorisation, considering the specific disadvantages to visitors, and held that the lack of prior consent of the visitors was the same as the socially accepted advertisements.

The five justices were unanimous in their opinions, and there were no supplementary or dissenting opinions.

In response to the Supreme Court judgment, some commentators have speculated about what the outcome would be if newspapers and news agencies ceased displaying advertisements and instead covered the running cost of their own sites with unauthorised mining (Emeritus Professor Sonoda). Others have pointed out the possibility that the judgment might differ if the mining program significantly consumed the CPU and memory.