Муҳтарам Зиё М. Фароқий
халқаро ҳакам, Америка Қўшма Штатлари, Колумбия округи округ суди (АҚШ)

КРИПТОВАЛЮТА: ТАҲЛИЛ, КУЗАТУВ, ОЛИБ ҚЎЙИШ

Достопочтенный Зия М. Фаруки
Мировой судья, США, Окружной суд округа Колумбия (США)

КРИПТОВАЛЮТА: АНАЛИТИКА, ОТСЛЕЖИВАНИЕ, ИЗЪЯТИЕ

Hon. Zia M. Faruqui
United States Magistrate Judge, U.S. District Court for the District of Columbia (USA)

CRYPTOCURRENCY: ANALYTICS, TRACING, SEIZING

When I used to work at the US Department of Justice for 12 years and I was involved in to international cyber and national security investigations. We conducted an investigation of the website: “Welcome to video” – the site was run for the purpose of child exploitation. After the year of investigation and international cooperation with many countries we took down the site on dark net. This was the largest dark net child pornography website.

As you know, the dark web is not what we see in regular web. Dark web is an unindexed Internet that requires a specialized software which is not illegal in the US to have. It is actually made by the US government called Onion Router to provide secure communications. The Onion Router helps you to navigate unnavigable portion of the Internet. If you use Yahoo or Google in regular internet to able to navigate – the dark net has no “street signs” or “street lights”. You would only be able to know which “house” to go to if you memorize the route. You go out of the highway, you go down three blocks, you turn left, then you turn right at the next street and go to the third house (all houses look the same) and you knock on the door four times. Thus, it is very difficult to find these types of websites.

Our investigation started in August 2017 and it had been continued on December 2017 until the present – clients of the website were the subject of international enforcement actions and arrest. In March 2018 we took down the person who was operating the website and the server. There had been 340 worldwide arrests, it involved 38 countries, we rescued 25 children who were being harmed.

The website is very non-descript; it shows the prices in bitcoin. Each person had dynamic cryptocurrency wallets, so there was not one static one – this what we had seen in another investigation – person had to have his/her own wallet.

The purpose of that is to avoid one general bank account, but to create a separate bank account for each transaction of each person – it creates logistical headache for the administrator / the owner who is receiving the funds, because they, instead of having one bank account – they have to make 50, 100 or in this case – thousands of different accounts. It does make tracing much more difficult. There are also numerous cryptocurrency exchanges that the person suggested to get money from. The website indicated whether you can either upload child exploitation content (CEC material) and you get points for that. More people download your video – more points you get. The administrator of the site insured that there was a new content, so people could either upload videos to get points or could buy the videos with Bitcoin under the assumption that tracing a Bitcoin was impossible. The website indicated that they didn't want any adult pornography, so primarily the website was dedicated to spread child pornography (mostly children under 5 y.o.) – really terrible and quite offensive conduct.

The way to close down the site required analytical software (the one that we used called TRM Labs) The software is like a calculator: you can do math on the sheet of paper and it will take a lot of time, or you can use a calculator and it will allow you to do the math much more quickly. The software helped to identify individual dynamic wallets that was associated with "Welcome to video" website and the places where the money came from. The question is: where does the money go? We wanted to know, who is running the website, with the idea that we could arrest that person and find the customers that were harming children.

We identified clients by going to exchanges that customers were engaged in by sending money to "Welcome to video". There was a great cooperation throughout the world. One of the great things about the cryptocurrency is – unlike traditional banks, where they may not answer international requests for assistance quickly – cryptocurrency exchanges want to stamp out illicit users. They don't want Bitcoin to be the tool for child exploitation or terroristic finance – they want to be a stable financial market. As investigators we told them about the customers – they helped us and assisted us through the international cooperation with direct assistance. TRM Software even showed us how we can get in touch with the exchange and assistance.

Thus, we sent the request to all crypto-exchanges and at the same time we noticed that the most of money was going to bit-com (exchange based in South Korea). We reached out to them and had a visit to South Korea and met with their compliance team.

The great thing about cryptocurrency is that it is completely visible, unlike if money went from HSBC to a person and then it went to another bank that would say: "We have no idea who is getting the money." Because all transactions were on the block chain they were able to see all exchanges of sending money to the addresses that were going then to bit-com.

The information that we've got from the above consisted of the user's ID, register name, email address, their full name, their state ID number, their home address and birthdate, IP address, etc. – extremely valuable information that allowed us to know who the customers of the website were.

Among the customers we identified two active federal law enforcement agents, a teacher at high school (assistant principal), two school IT specialists, daycare provider, paramedic, dentist, former senate staffer and staff to former Vice-President of US.

IRS agents have opened undercover accounts and send cryptocurrency to trace the money through software that led us to South Korea. We found the first uploader of the "Welcome to video" website and he used the word "admin", that made us think that he was an administrator of the website. Then, through finding common usernames and common IP addresses, usage of linguistics to identify who this particular user might be.

Next, we went using court authorized search warrants to be able to find email accounts of the person that we believed was the user – administrator of the website. We revealed his user ID card as well as his photos.

The hard part of the dark net investigation is not proving that there was a crime, but attribution – who is an actual person and how do you prove that is the person. We use search warrants – a tool that any foreign country can ask a US assistance. At the courts of Washington, DC we receive all Mutual legal assistance requests through the Department of Justice's Office of International Affairs. When foreign countries identify email addresses, related to their investigation, to get the content of those emails – you can get that by sending the request to the USA and then free of cost of this information will be provided to you.

Korean police found the base to search this person's house, they took down the door and they found that he was on computer there with the website open. Then we have seized the website, and started the process of arresting customers around the world.