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, 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 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 the dark web. This was the largest dark net child pornography website.

As you know, the dark web is not what we see on the regular web. Dark web is an unindexed internet that requires a specialized software which is not illegal in the US. It was actually commissioned by the US government to provide secure communications called the Onion Router. It helps you navigate unnavigable portion of the internet. It’s like the dark web has no street signs or streetlights that are Google and Yahoo for the regular web. You would only be able to know which “house” to go to if you memorize the route. It is very difficult to find these types of websites.

Our investigation started in August 2017 until the present. Clients of the website have been the subject of international enforcement actions and arrests. In March 2018 we took down the person who was operating the website and the server. There have 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, which allows users to avoid one general bank account and create a separate bank account for each transaction. This is a logistical headache for the administrator/the owner who receives the funds, because they too need 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 the inflow of new content, so people could upload videos for points or buy videos with Bitcoin under the assumption that tracing Bitcoin was impossible. The website indicated that they don't want any adult pornography, so primarily the website was dedicated to spread child pornography (mostly children under 5) – really terrible and quite offensive conduct.

The way to close down the site required analytical software (we used TRM Labs) which works like a calculator – you can do math with pen and paper, but it will take a long time, or you can use a calculator and get results much faster. The software helped identify individual dynamic wallets associated with the 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 was 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. We had great global cooperation. One of the great things about 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 terrorism financing – they want to be a stable financial market. When 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. We sent a request to all crypto-exchanges and at the same time we noticed that most of the money was going to bit-com (exchange based in South Korea). We went to South Korea and met with their compliance team.

The great thing about cryptocurrency is that it is completely visible, unlike if money was going from HSBC to a person and then it went to another bank, we would have no idea who was receiving the money. Because all transactions were on the blockchain they were able to see all exchanges that were coming to bit-com.

The information we received were user IDs, register names, email address, their full names, state ID numbers, home addresses, birthdates, IP address, etc. – extremely valuable information that allowed us to know who the customers of the website were. Among them we identified two active federal law enforcement agents, a teacher at the 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 the cryptocurrency to trace the money through the software that led us to South Korea. We found the first uploader to Welcome to video and he used the word "admin", that made us think that he was an administrator of the website. Then, through finding common usernames, common IP addresses and linguistic identifiers we could identify this first user. Through court ordered warrants we were then able to access email accounts of this person who turned out to be the administrator of the website. We revealed his user ID card as well as his photo.

The hard part of dark web investigation is not proving that there was a crime, but attribution – who is the perpetrator and proving they are the perpetrator. We use search warrants – a tool that any foreign country can ask US assistance with. At the courts of Washington, DC we receive all the 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 this information will be provided to you.

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