UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Holding a Criminal Term
Grand Jury Sworn in May 7, 2019

UNITED STATES OF AMERICA	Case: 20-cr-0065 Assigned To : Judge Dabney L. Friedrich Assign. Date : 3/5/2020 Description: INDICTMENT (B) Related Case No. 18CR243 (DLF)
v.	
MICHAEL RAHIM MOHAMMAD,	**18 U.S.C. § 2252(a)(2)** **(Distribution of Child Pornography)**
Defendant.	
	18 U.S.C. § 1465 **(Production and Transportation of Obscene Matters For Sale or Distribution)**
	18 U.S.C. § 1466 **(Engaging In The Business of Selling or Transferring Obscene Matter)**
	18 U.S.C. § 1956(a)(2)(A) **(Laundering of Monetary Instruments)**
	FORFEITURE: **21 U.S.C. § 853; 18 U.S.C. § 982;** **18 U.S.C. § 1467 and 2253**
	UNDER SEAL

INDICTMENT

The Grand Jury charges that:

At times material to this Indictment:

DEFINITION OF TERMS

The Tor Network

1. Tor was a computer network which anonymized Internet activity by routing a user's communications through a global network of relay computers (or proxies), thus effectively masking the internet-protocol ("IP") address of the user.

2. An "IP address" was a unique numeric address (used by computers on the internet) that is assigned to properly direct internet traffic. A publically visible IP address could allow for the identification of the user and his/her location.

3. To access the Tor network, a user had to install freely available Tor software, which relayed only the IP address of the last relay computer (the "exit node"), as opposed to the user's actual IP address. There was no practical method to trace a user's actual IP address back through those Tor relay computers.

4. The Tor network made it possible for a user to operate a special type of website, called "hidden services," which used a web address that is comprised of a series of 16 algorithm-generated characters (such as "asdlk8fs9dflku7f") followed by the suffix ".onion." Websites, including hidden services, had system administrator(s) (also called the "admin(s)") who were responsible for overseeing and operating these websites.

Bitcoin and Ethereum

5. Bitcoin (BTC) and Ether (ETH) are pseudonymous virtual currencies. Although

transactions are visible on a public ledger, each transaction is referenced by a complex series of numbers and letters (as opposed to identifiable individuals) involved in the transaction. The public ledger containing this series of numbers and letters is called a blockchain. This feature makes BTC and ETH pseudonymous; however, it is often possible to determine the identity of an individual involved in BTC and ETH transactions through several different tools. For this reason, many criminal actors who use BTC and ETH to facilitate illicit transactions online (*e.g.,* to buy and sell drugs or other illegal items or services) look for ways to make their transactions even more anonymous.

6. BTC/ETH were not issued by any government, bank, or company, but rather were controlled through computer software.

7. BTC/ETH fluctuated in value. As of March 5, 2020: one BTC was worth approximately $9,102.65, and one ETH was worth approximately $232.41.

8. BTC/ETH addresses are unique tokens; however, BTC/ETH are designed such that one person may easily operate many such accounts. Like an email address, a user can send and receive BTC/ETH with others by sending BTC/ETH to a BTC/ETH address. People commonly have many different addresses, and an individual could theoretically use a unique address for every transaction in which they engage.

9. To spend BTC/ETH held within a BTC/ETH address, the user must have a private key, which is generated when the BTC/ETH address is created. Similar to a password, a private key is shared only with the BTC/ETH-address key's initiator and ensures secured access to the virtual currency. Consequently, only the holder of a private key for a BTC/ETH address can spend BTC/ETH from the address. A BTC user can also spend from multiple BTC addresses in one

transaction; for example, five addresses each holding five BTC can collectively send 25 BTC in a single transaction.

10. Although generally, the owners of BTC/ETH addresses are not known unless the information is made public by the owner (for example, by posting the address in an online forum or providing the BTC/ETH address to another user for a transaction), analyzing the public transaction ledger can sometimes lead to identifying both the owner of an address and any other accounts that the person or entity owns and controls.

11. BTC/ETH are often transacted using a virtual currency exchange, which is a virtual currency trading and storage platform. An exchange typically allows trading between the U.S. dollar, other foreign currencies, BTC, ETH, and other virtual currencies. Many virtual currency exchanges also store their customers' virtual currencies. These exchanges act as money services businesses and are legally required to conduct due diligence of their customers and have anti-money laundering checks in place. Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act, codified at 31 U.S.C. § 5311 *et seq.*, and must collect identifying information of their customers and verify their clients' identities.

Blockchain Analysis

12. Once the sender's transaction announcement was verified, the transaction was added to the blockchain.

13. The blockchain was a decentralized, public ledger that logged every BTC/ETH transaction.

14. Law enforcement can identify the owner of a particular BTC/ETH address by analyzing the blockchain. The analysis can also reveal additional addresses controlled by the same

individual or entity. For example, a user or business may create many BTC addresses to receive payments from different customers. When the user wants to transact the BTC that it has received (for example, to exchange BTC for other currency or to purchase goods or services), it may group those addresses together to send a single transaction. Law enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions. These companies analyze the blockchain and attempt to identify the individuals or groups involved in the virtual currency transactions. Specifically, these companies create large databases that group transactions into "clusters" through analysis of data underlying the virtual currency transactions.

DARKSCANDALS WEBSITES

The DarkScandals Darknet and Clearnet Websites

15. Darknet markets are typically commercial websites operating as hidden services using Tor, which primarily function as black markets in which users engage in selling or brokering transactions involving products, such as drugs, unlicensed pharmaceuticals, cyber-arms, weapons, counterfeit currency, stolen credit-card details, forged documents, or, as pertinent to the instant investigation, obscene materials, including child pornography. BTC is one of the most common methods of payment for products or services bought and sold within darknet markets.

16. A "clearnet" website is accessible using traditional Internet browsers, such as Internet Explorer or Safari. These websites use traditional designations, such as ".com" or ".co."

17. The DarkScandals site was available on the darknet ("DarkScandals Darknet") and the clearnet ("DarkScandals Clearnet") (collectively the "DarkScandals Sites").

18. The DarkScandals Clearnet site began in or about 2012 as darkscandals.com, which

subsequently transitioned to darkscandals.co in or about February 2019 after the original site was the subject of complaints.

19. The DarkScandals Darknet and DarkScandals Clearnet sites were virtually identical and largely offered the same service: directing customers on how to obtain obscene content, including videos that depicted sexual assault and child pornography.

20. MICHAEL RAHIM MOHAMMAD, the defendant, was the administrator of the DarkScandals Sites, which he began operating in or about 2012.

Operation of the DarkScandals Sites

21. The DarkScandals Sites advertised that it offered "real blackmail, rape and forced videos of girls all around the world."

22. The DarkScandals Sites offered users two ways to access content, which was delivered in "packs" by the defendant. Users could either:

a. pay for the packs; or

b. upload new videos, which the defendant curated, and receive the packs for free.

23. The defendant advertised that the packs contained approximately 2,000 videos and images.

Uploading Content to the DarkScandals Sites

24. The DarkScandals Sites included specific rules for the video uploads to the DarkScandals Sites, including the following:

- "Videos with real rape/forced (agains [sic] will)"
- "Videos with real blackmail (would be better with chatlog)"
- "Real groped girls (not acted videos) (extreme kind)"

- "real busted girl doing some nasty stuff (like busted sex with animal or something extreme)"
- "real underground sold slave girl videos"
- "This video can not be found on other (easily) accessible sites"
- "Your video is not already in the pack"
- "Only videos with face (of girl) in it will be accepted"
- "We prefer own made material (if you have some material where you are also on it, and you want yourself out of the video, send the original, we will edit it how you want it and put it in the packs)"
- "Please do NOT send videos with dead stuff, fake, amateur, masturbation or acted movies!"

25. The defendant advertised on the DarkScandals Sites that he used three different anonymous data-transfer services (which allow users to store and share files without providing any identifying information to the service) to receive uploads of customer's obscene content.

26. The defendant advertised that he would respond to customers after they uploaded content with an email in 24 to 48 hours that contained a download link that allowed the customer to download the packs.

27. The defendant rejected uploads if the videos were inconsistent with the obscene content on the site or were already in the packs. For example, on or about December 1, 2013, the defendant informed a customer that the defendant had rejected the customer's uploaded video because "its [sic] just acted, we don't accept video's [sic] like that for the packs." The defendant signed this email as "Dark," which was one of his online monikers.

28. On or about September 29, 2014, the defendant created an account on one of these anonymous data-transfer services, which he used to receive obscene content.

Payments to the Defendant to Access the DarkScandals Sites' Content

29. Prior to in or about November 2013, the DarkScandals Sites directed users to transfer fiat currency to an account associated with the site.

30. In or about November 2013, the DarkScandals Sites began directing customers to send payments of BTC to an address beginning in 1Fiptr ("1Fiptr") to access the obscene content. The defendant created the 1Fiptr address.

31. The defendant subsequently directed payments to additional BTC addresses and one ETH address.

32. The DarkScandals Sites instructed customers to send proof of their BTC/ETH payments to an encrypted email address provided on the DarkScandals Sites.

33. Some customers would instead send BTC/ETH payments to this encrypted email address. For example, on or about March 26, 2016, a customer in Washington D.C. sent an email to the defendant with a link to accept payment of 0.15 BTC for the purchase of the DarkScandals packs.

34. The DarkScandals Sites received approximately 1,650 deposits totaling 188.6631 BTC (approximately valued, as of March 1, 2020, at $1.6 million) and 26.724 ETH (approximately valued at $5,730.96).

35. The defendant, using his own identifying information, created accounts at banks and virtual currency exchanges to covert these funds into fiat currency.

Undercover Purchases

36. On or about February 13, 2018, law enforcement, acting in an undercover capacity, sent 0.0197777 BTC ($25.27) to the 1Fiptr address.

37. On April 20, 2018, law enforcement, acting in an undercover capacity in Washington, D.C., clicked on a download link in an email from "bitcoin@darkscandals.com," which email was hosted by an anonymous email service provider that was located in Germany.

38. A review of the content downloaded by law enforcement in Washington, D.C., revealed that the DarkScandals Sites were distributing child sexual exploitation material and obscene material, such as:

a. a video titled "pinkRubband.avi," which was identified by the National Center for Missing and Exploited Children as depicting a 14-year-old girl who was extorted into filming herself engaged in sexually explicit conduct. Specifically, the minor, while in front of her computer's web camera, exposed and rubbed her genitalia and subsequently penetrated her vagina with her fingers.

b. a video titled "Sierra_Blackmail_Video.avi," which was identified by the National Center for Missing and Exploited Children as depicting a child who was between the ages of 14 and 17 years old during the time that she was extorted into filming herself engaged in sexually explicit conduct. Specifically, the minor, who appeared to be closer to 14 years old at the time of the video, exposed and touched her genitalia and subsequently penetrated her vagina with a pink pencil while in front of her computer's

web camera.

c. a video titled "the regret of a analwhore.avi," which depicted a woman purportedly consenting to anal sex but then indicating her desire to stop. The man refused and forced anal sex as the woman screamed in pain and pled with him to stop.

d. a video titled "stick rape.mp4," which depicted an unconscious and unmoving woman being vaginally penetrated with both ends of a baseball bat and causing injury to the woman's genitalia; and

e. a video titled "Drunk_passed_out_girl_violated_with_bottle.3gp," which depicted an unconscious and unmoving woman being vaginally penetrated with a vodka bottle while the camera zoomed in on the act of penetration.

39. On or about March 2, 2020, law enforcement, acting in an undercover capacity while in Washington D.C., sent 0.021269 BTC ($189.27) to an address beginning in 1MFrs ("the 1MFrs address") associated with the DarkScandals Sites. The 1MFrs address was among those to which the DarkScandals Sites directed users that they could make payments.

40. On or about March 4, 2020, law enforcement, acting in an undercover capacity while in Washington D.C., communicated with the defendant about this payment.

Defendant's Control of the DarkScandals Sites

41. On or about June 29, 2014, the defendant paid .09 BTC to a service provider in the United States to host the DarkScandals Darknet site.

42. On or about July 7, 2014, the defendant received page view numbers for the DarkScandals Clearnet site, which showed over 13,000 unique visit to the site in one week.

43. The defendant paid into service providers in the United States for infrastructure used by the DarkScandals Clearnet site using a financial account registered in the defendant's name.

44. The defendant's personal email account was accessed routinely with IP addresses located in the Netherlands and contained communications regarding the operation of the DarkScandals Sites, such as administering BTC payments and communicating with domain hosting services known to be used by the DarkScandals Clearnet Site.

45. On or about January 18, 2018, the defendant received a receipt for the purchase of an adult video script streaming service. The defendant subsequently sought assistance from the adult video script service in implementing the script into the DarkScandals Clearnet Site. The defendant identified himself as the administrator of the site in this communication.

46. For a period of time in or about 2018 and 2019, the DarkScandals Clearnet Site offered the obscene content via a pay for streaming service.

47. On or about April 3, 2018, the defendant received a warning that the content on DarkScandals Clearnet Site contained "violence and rape" and was asked to remove it. The specifically identified videos were:

i. "moslim-girl-raped-while-filmed-by-friend"

ii. "indian-girl-raped-while-crying"

iii. "crying-girl-stripped-and-gangrapped"

iv. "indian-girl-raped-outside"

48. The defendant did not remove the above content.

49. In or about February 2019, the defendant transitioned the DarkScandals Clearnet

site to darkscandals.co.

50. On or about February 5, 2019, the defendant made a payment into the United States for the hosting service used for DarkScandals Clearnet.

51. In or about March 2019, the defendant started to receive alerts for deposits to the 1MFrs BTC address, which address was listed on the DarkScandals Sites.

COUNT ONE

52. Paragraphs 1 through 51 are incorporated here.

53. On or about April 20, 2018, within the District of Columbia and elsewhere, the defendant, MICHAEL RAHIM MOHAMMAD, did knowingly distribute any visual depiction, to include video file "Pinkrubband Video," using any means and facility of interstate and foreign commerce, including by computer, where the visual depiction involved the use of a minor engaging in sexually explicit conduct as defined in Title 18, United States Code, Section 2256(2)(A), and such visual depiction is of such conduct.

(Distribution of Child Pornography, in violation of Title 18, United States Code, Section 2252(a)(2))

COUNT TWO

54. Paragraphs 1 through 51 are incorporated here.

55. On or about April 20, 2018, within the District of Columbia and elsewhere, the defendant, MICHAEL RAHIM MOHAMMAD, did knowingly distribute any visual depiction, to include video file "Sierra_Blackmail_Video," using any means and facility of interstate and foreign commerce, including by computer, where the visual depiction involved the use of a minor engaging in sexually explicit conduct as defined in Title 18, United States Code, Section 2256(2)(A), and

such visual depiction is of such conduct.

(Distribution of Child Pornography, in violation of Title 18, United States Code, Section 2252(a)(2))

COUNT THREE

56. Paragraphs 1 through 51 are incorporated here.

57. On or about April 20, 2018, within the District of Columbia and elsewhere, the defendant, MICHAEL RAHIM MOHAMMAD, knowingly caused to be transported in interstate and foreign commerce an obscene matter, and used a facility of interstate and foreign commerce, for the purpose of selling and distributing an obscene matter, that is "the regret of a analwhore.avi," a video on the DarkScandals Sites that depicted forced anal penetration.

(Production and Transportation of Obscene Matters For Sale or Distribution, in violation of Title 18, United States Code, Section 1465)

COUNT FOUR

58. Paragraphs 1 through 51 are incorporated here.

59. On or about April 20, 2018, within the District of Columbia and elsewhere, the defendant, MICHAEL RAHIM MOHAMMAD, knowingly caused to be transported in interstate and foreign commerce an obscene matter, and used a facility of interstate and foreign commerce, for the purpose of selling and distributing an obscene matter, that is "stick rape.mp4," a video on the DarkScandals Sites that depicted a non-consenting woman being vaginally penetrated, that is, raped, by both ends of a baseball bat while unconscious.

(Production and Transportation of Obscene Matters For Sale or Distribution, in violation of Title 18, United States Code, Section 1465)

COUNT FIVE

60. Paragraphs 1 through 51 are incorporated here.

61. On or about April 20, 2018, within the District of Columbia and elsewhere, the defendant, MICHAEL RAHIM MOHAMMAD, knowingly caused to be transported in interstate and foreign commerce an obscene matter, and used a facility of interstate and foreign commerce, for the purpose of selling and distributing an obscene matter, that is "Drunk_pass_out_girl_violated_ with_bottle.3gp," a video on the DarkScandals Sites that depicted a non-consenting woman being vaginally penetrated, that is, raped, by a vodka bottle while unconscious.

(Production and Transportation of Obscene Matters For Sale or Distribution, in violation of Title 18, United States Code, Section 1465)

COUNT SIX

62. Paragraphs 1 through 51 are incorporated here.

63. On or about April 20, 2018, within the District of Columbia and elsewhere, the defendant, MICHAEL RAHIM MOHAMMAD, engaged in the business of selling and transferring obscene matter, that is obscene matter on the DarkScandals Sites, and knowingly received and possessed with intent to distribute this obscene matter, which has been shipped and transported in interstate and foreign commerce.

(Engaging In The Business of Selling or Transferring Obscene Matter, in violation of Title 18, United States Code, Section 1466)

COUNT SEVEN – COUNT NINE

64. Paragraphs 1 through 51 are incorporated here.

65. On or about the dates below within the District of Columbia and elsewhere, the defendant, MICHAEL RAHIM MOHAMMAD, caused the transmission and transfer, of a monetary instrument and funds, in the amounts described below, from a place in the United States, that is, Washington, D.C., to or through a place outside the United States, that is The Netherlands, with the intent to promote the carrying on of specified unlawful activity, that is, violations of: section 2252 (relating to child pornography, where the child pornography contains a visual depiction of an actual minor engaging in sexually explicit conduct), dealing in obscene matter, and violation of section 1465 (producing and transporting obscene matter).

Count	Date (On or about)	Amount
SEVEN	March 26, 2016	0.15 BTC
EIGHT	February 13, 2018	0.0197777 BTC
NINE	March 2, 2020	0.021269 BTC

(**Laundering of Monetary Instruments**, in violation of Title 18, United States Code, Section 1956(a)(2)(A))

FORFEITURE ALLEGATION

The Grand Jury further finds by probable cause that:

1. Upon conviction of any the offenses alleged in Count One and Count Two, the defendant shall forfeit to the United States any visual depiction described in Title 18, United States Code, Sections 2251, 2252, or 2260, or any book, magazine, periodical, film, videotape, or other

matter which contains any such visual depiction, which was produced, transported, mailed, shipped or received in violation of Title 18, United States Code, Chapter 110; any property, real or personal, constituting or traceable to gross profits or other proceeds obtained from this offense; and any property, real or personal, used or intended to be used to commit or to promote the commission of this offense or any property traceable to such property, pursuant to Title 18, United States Code, Section 2253(a). The United States will also seek a forfeiture money judgment against the defendant equal to the value of any property, real or personal, constituting or traceable to gross profits or other proceeds obtained from these offenses; and any property, real or personal, used or intended to be used to commit or to promote the commission of these offenses or any property traceable to such property.

2. Upon conviction of any the offenses alleged in Count Three through and Count Five, the defendant shall forfeit to the United States: (1) any obscene material produced, transported, mailed, shipped, or received in violation of this chapter; (2) any property, real or personal, constituting or traceable to gross profits or other proceeds obtained from such offense; and (3) any property, real or personal, used or intended to be used to commit or to promote the commission of such offense, pursuant to Title 18, United States Code, Section 1467. The United States will also seek a forfeiture money judgment against the defendant equal to the value of any property, real or personal, constituting or traceable to gross profits or other proceeds obtained from such offense, and any property, real or personal, used or intended to be used to commit or to promote the commission of such offense

3. Upon conviction of the offenses alleged in Count Seven through Count Nine of this Indictment, the defendant shall forfeit to the United States any property, real or personal, involved

in these offenses, or any property traceable to such property pursuant to Title 18, United States Code, Section 982(a)(1). The United States will also seek a forfeiture money judgment for a sum of money equal to the value of any property, real or personal, involved in these offenses, and any property traceable to such property.

4. The specific property subject to forfeiture includes:

a. Darkscandals.com;

b. Darkscandals.co;

c. Bitcoin address: 1Fiptr7bQdh6754yWzfmuytEe6ekihZ8V6;

d. Bitcoin address: 12kQwWjBkxHjRmCQBKjReAERu9SnzU6u8Y;

e. Bitcoin address: 1MFrsV3Y6n8qDW7CHVJMeLbkEqyhvPvurA; and

f. Ethereum address: 0x1c57BAC4757a8D46131776eA52706F4d3eb00fd1.

5. If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or

e. has been commingled with other property that cannot be divided without difficulty;

the defendant shall forfeit to the United States any other property of the defendant, up to the value of the property described above, pursuant to 21 U.S.C. § 853(p).

(**Criminal Forfeiture**, pursuant to Title 18, United States Code, Sections 2253(a), 1467, and 982(a), and Title 21, United States Code, Section 853(p)).

A TRUE BILL

_____
FOREPERSON

Timothy J. Shea (KK
Attorney of the United States
in and for the District of Columbia