FILED

Jun 07 2021

SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

3:21-mj-70945-LB

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEIZURE WARRANT

I, [redacted], am an investigative or law enforcement officer of the United States, within the meaning of 18 U.S.C. § 2510(7), and I am empowered by law to conduct investigations of and to make arrests for offenses enumerated in 18 USC §§ 371, 1030, and 1956, among others. Being first duly sworn, I hereby depose and state as follows:

INTRODUCTION

1. This affidavit is in support of a seizure warrant for approximately 63.7 bitcoins (the "Subject Funds") accessible from the following cryptocurrency address (the "Subject Address"): XXXXXXXXXXXX950klpjcawuy4uj39ym43hs6cfsegq.

AGENT BACKGROUND

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since [redacted]. I am currently assigned to the Cyber Crimes Squad of the FBI's San Francisco Field Division. I successfully completed the 21 weeks of New Agent Training at the FBI Academy in Quantico, Virginia in [redacted]. During that time, I received training in physical surveillance, legal statutes and procedures, financial investigations, money laundering techniques, asset identification, forfeiture and seizure, confidential source management, and electronic surveillance techniques. Since joining the FBI, I have investigated violations of federal law to include those related to criminal cyber intrusion violations.

3. I am currently assigned to work primarily cases involving criminal intrusion violations. As an FBI agent, I am authorized to investigate violations of federal law, and execute warrants issued under the authority of the United States. I received my Juris Doctor in [redacted] and am a member in good standing with the [redacted]. I have experience with Federal criminal law, the Federal Rules of Evidence, and the Federal Rules of Criminal Procedure. I have also received specialized training and instruction in the field of investigation in computer-related crimes, and

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

have had the opportunity to conduct, coordinate, and participate in numerous investigations relating to computer-related crimes. I have participated in the execution of numerous search warrants conducted by the FBI and have participated in the seizure of computer systems.

4. This affidavit is submitted pursuant to Rule 41 of the Federal Rules of Criminal Procedure, and 18 U.S.C. §§ 981(a)(1)(A) and (C), 981 (b)(1) and (2), 982(a)(1) and (b)(1), and 1030(i) for the issuance of a warrant (the "Seizure Warrant") to seize and forfeit the Subject Funds.

5. The facts and information contained in this affidavit are based upon my personal knowledge, as well as information from other law enforcement officers involved in this investigation. Statements made by witnesses and other individuals referenced in this affidavit have been paraphrased. While this affidavit does not contain every piece of evidence discovered to date, it does not omit evidence that would defeat the probable cause established herein.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to seize the property described above.

LEGAL AUTHORITY FOR SEIZURE

7. Title 18 U.S.C. §§ 981(a)(1)(C) and 1030(i) provide for the criminal and civil forfeiture of any property which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1030 (Computer Hacking) and any personal property that was used or intended to be used to commit or to facilitate the commission of such violations.

8. Title 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1) provide for the criminal and civil forfeiture of any property, real or personal, "involved in" a violation of 18 U.S.C. § 1956 (Money Laundering), or any property traceable to such property.

9. 18 U.S.C. § 981(b) provides for the seizure of property subject to civil forfeiture. 18 U.S.C. § 981(b)(3) further provides:

> Notwithstanding the provisions of rule 41(a) of the Federal Rules of Criminal Procedure, a seizure warrant may be issued pursuant to this subsection by a judicial officer in any district in which a forfeiture action against the property may be filed under section 1355(b) of title 28, and may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

service in accordance with any treaty or other international agreement. Any motion for the return of property seized under this section shall be filed in the district court in which the seizure warrant was issued or in the district court for the district in which the property was seized.

10. Title 18, U.S.C. § 1030(a)(2)(C), makes it a crime for an individual to intentionally access a computer without authorization or exceed authorized access, and thereby obtain information from a protected computer. The offense is a felony if "committed for purposes of commercial advantage or private financial gain."

11. Title 18, U.S.C. § 1030(a)(5)(A), makes it a crime for an individual to knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer.

12. Title 18, U.S.C. § 1030(a)(7)(C), makes it a crime to intentionally extort any person any money or other thing of value, transmit in interstate or foreign commerce any communication containing any demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion.

13. Title 18 U.S.C. § 1956(a)(1), makes it a crime to engage or attempt to engage in a financial transaction with the proceeds of a specified unlawful activity: (1) with the intent to promote the carrying on of a specified unlawful activity; (2) with the intent to evade taxes; (3) knowing the transaction is designed, in whole or in part, to conceal or disguise the source, origin, nature, ownership, or control of the proceeds; or (4) knowing the transaction is designed, in whole or in part, to avoid a transaction reporting requirement.

14. Title 18 U.S.C. § 1956(h) makes it a crime to conspire to commit any of the offenses set forth in 18 U.S.C. § 1956.

15. One of the chief goals of forfeiture is to remove the profit from crime by separating the criminal from his or her dishonest gains. *See* United States v. Newman, 659 F.3d 1235, 1242 (9th Cir. 2011); United States v. Casey, 444 F.3d 1071, 1073 (9th Cir. 2006). To that end, if property appreciates in value or earns interest, any appreciation or interest is subject to forfeiture. *See* United States v. Betancourt, 422 F.3d 240, 250 (5th Cir. 2005); United States v. Hawkey, 148 F.3d 920, 928 (8th Cir. 1998).

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DEFINITIONS

16. I know from my training and experience as a Special Agent with the FBI that the following definitions apply to the activity discussed in this affidavit:

17. **Bitcoin**: Bitcoin is a type of cryptocurrency, circulated over the Internet as a value that substitutes for currency. Bitcoin is not issued by any government, bank, or company, but rather is generated and controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin is just one of many types of cryptocurrency.[1]

18. **Bitcoin address**: Bitcoin addresses are the particular virtual locations to which bitcoin are sent and received. A Bitcoin address is analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers.

19. **Private Key**: Each Bitcoin address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address's private key can authorize a transfer of Bitcoin from that address to another Bitcoin address.

20. **Bitcoin Wallet**: A Bitcoin wallet is a software application that interfaces with the Bitcoin blockchain and generates and stores a user's addresses and private keys. A Bitcoin wallet also allow users to send and receive bitcoins. Multiple addresses can be stored in a wallet.

21. **Blockchain**: All Bitcoin transactions are recorded on what is known as the Bitcoin blockchain. The blockchain is essentially a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction. The blockchain updates approximately six times per hour and records every Bitcoin address that has ever received bitcoin and maintains records of every transaction and all the known balances for each Bitcoin address. The blockchain is visible online to everyone.

---

[1] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) or BTC to label units of the cryptocurrency. That practice is adopted here.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

22. **Blockchain Explorer**: A blockchain explorer is software that uses API and blockchain nodes to draw data from a blockchain and uses a database to arrange and present the data to a user in a searchable format. These explorers are online tools that operate as a blockchain search engine that allows users to search for and review transactional data for any addresses on a particular blockchain.

FACTS SUPPORTING PROBABLE CAUSE

A. BACKGROUND

23. The FBI is investigating suspected violations of Title 18, United States Code, Section 1030(a)(2)(C), Unauthorized Access to a Protected Computer to Obtain Information, Title 18, United States Code, Section 1030(a)(5)(A), Intentional Damage to a Protected Computer, Title 18, United States Code, Section 1030(a)(7)(C), Extortion Involving Computers, among other statutes, and Title 18, United States Code, Section 1956 (Money Laundering).

24. Ransomware is a type of malicious software that infects a computer system and restricts a user from accessing that system or the files contained therein through encryption.[2] These files and systems remain encrypted until a ransom is paid, at which time a decryptor, or a tool allowing for the decryption of files, is provided. Typically, threat actors utilizing ransomware will breach a network, exfiltrate data from the victim's network, plant the malicious software to encrypt data, and demand a ransom. If the ransom is not paid, the threat actor often threatens to publish the stolen data online.

[2] Encryption is the method by which information is converted into secret code that hides the information's true meaning. By encrypting files on a system, a threat actor can make the files unreadable and unusable until the encryption is reversed, or the information is decrypted.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.