

**ORIGINAL**

FILED IN OPEN COURT  
U.S.D.C. Atlanta

SEP 19 2017

James N. Hatten, Clerk  
By: Deputy Clerk *CHM*

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION

UNITED STATES OF AMERICA

v.

JOSHUA POLLOSO EPIFANIOU,  
a/k/a Charley Sullivan,  
a/k/a Chary Malatan,  
a/k/a Richard Charley

Criminal Indictment

No. **1:17CR327**

Under Seal

THE GRAND JURY CHARGES THAT:

**COUNT ONE**

(Wire Fraud Conspiracy)

1. Beginning on an unknown date, but at least by in or about October 2014, and continuing through in or about November 2016, in the Northern District of Georgia and elsewhere, the defendant, JOSHUA POLLOSO EPIFANIOU, a/k/a Charley Sullivan, a/k/a Chary Malatan, a/k/a Richard Charley, with others known and unknown to the Grand Jury, did knowingly conspire to devise and intend to devise a scheme and artifice to defraud U.S.-based websites, and to obtain money and property from those websites, including the confidential personal identifying information of website users, by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing and attempting to execute such scheme and artifice, did with intent to defraud cause the transmission by means of wire communication in interstate

and foreign commerce of certain writings, signs, signals, pictures, and sounds, in violation of Title 18, United States Code, Section 1343.

**BACKGROUND**

2. At all times relevant to this Indictment:

a. Defendant JOSHUA POLLOSO EPIFANIOU, a/k/a Charley Sullivan, a/k/a Chary Malatan, a/k/a Richard Charley, was a resident of Nicosia, Cyprus. EPIFANIOU previously received payments from “bug bounty” programs for identifying and reporting network security vulnerabilities.

b. Turner Broadcasting System, Inc. (“Turner”) is an entertainment company headquartered in Atlanta, Georgia that is a division of Time Warner. Turner owns the sports news website, Bleacher Report, which is based in San Francisco, California. Turner maintains computer servers located in the Northern District of Georgia and other locations in the United States that contain user databases. These databases store personal identifying information of Bleacher Report users, including full names, email addresses, and account passwords. This user information was confidential and economically valuable business information for Turner, and the company stored the information on restricted, nonpublic servers in the United States.

c. Adafruit Industries (“Adafruit”) is a hardware company based in New York, New York that designs, manufactures, and sells electronics products. Adafruit maintains customer databases that store personal identifying information of its customers, including full names, email addresses, credit card numbers, and passwords. This customer information was confidential and

economically valuable business information for Adafruit, and the company stored the information on restricted, nonpublic servers in the United States.

d. Snagajob is an online employment website headquartered in Innsbrook, Virginia that provides a job search engine for users. Snagajob maintains user databases that store personal identifying information of its users, including email addresses and passwords. This user information was confidential and economically valuable business information for Snagajob, and the company stored the information on restricted, nonpublic servers in the United States.

e. Armor Games is a free online game publisher based in Irvine, California that offers users the ability to chat and create profiles. Armor Games maintains user databases that store personal identifying information of its users, including email addresses and passwords. This user information was confidential and economically valuable business information for Armor Games, and the company stored the information on restricted, nonpublic servers in the United States.

f. Bitcoin is a digital currency using cryptography to secure transactions and to control the creation of additional units of the currency. A bitcoin wallet permits account holders to send, receive, and manage their bitcoin. EPIFANIOW owned and controlled a bitcoin wallet maintained by the cryptocurrency wallet service, Blockchain.info, which is headquartered in Luxembourg.

**OBJECT OF THE CONSPIRACY**

3. It was the object of the conspiracy for defendant Defendant JOSHUA POLLOSO EPIFANIOU, a/k/a Charley Sullivan, a/k/a Chary Malatan, a/k/a Richard Charley, and his co-conspirators to gain access to the computer networks of at least five U.S.-based victims, steal personal identifying information from user and customer databases at the victim websites, and threaten public disclosure of the sensitive personal data unless the website operators paid a ransom. In a series of communications through an internet instant messaging service, EPIFANIOU stated in March 2017 that he was “hacking corps blackmail for \$\$” and “hacking, extortion, blackmailing, bluffing, I do all that [expletive] all in 1 year → \$350k.”

**MANNER AND MEANS OF THE SCHEME TO DEFRAUD**

4. The manner and means by which the scheme and artifice to defraud was sought to be accomplished included, among others, the following:

a. Defendant JOSHUA POLLOSO EPIFANIOU, a/k/a Charley Sullivan, a/k/a Chary Malatan, a/k/a Richard Charley, identified potential targets for his ransomware scheme by searching website traffic rankings published by Alexa Internet, Inc. to determine the size of the targets.

b. After identifying potential targets, EPIFANIOU obtained confidential user database records from the targets in two ways. For certain victims, including Armor Games and Adafruit, EPIFANIOU gained unauthorized access to the public website through a security vulnerability and injected malicious code into the website to exfiltrate user and customer data. For other victims, including Turner and Snagajob, EPIFANIOU obtained only a

portion of the victim website's user database from a co-conspirator who had breached the victim's networks and exfiltrated personal identifying information.

c. EPIFANIOU set up online email services in the name of an alias, including Charley Sullivan, Chary Malatan, and Richard Charley, to communicate with victims. EPIFANIOU also used proxy servers located abroad to log into the email addresses when sending messages to the victims.

d. Using the alias email accounts, EPIFANIOU sent email messages from Cyprus to the victim companies in the United States stating that he had downloaded their user database and would leak the contents of the database, including personal identifying information, to a public website if the victim website operators did not pay a ransom of thousands of dollars within hours. Even though EPIFANIOU obtained from his co-conspirator only a portion of the user database for certain victims, EPIFANIOU falsely represented that he exfiltrated the entire user database and would reveal the security vulnerability purportedly exploited to download the data.

e. When victim websites asked him for verification of the breach, EPIFANIOU sent files showing screenshots or other records obtained from the user databases. In one instance, EPIFANIOU paid a co-conspirator to text a message to Turner to demand the payment of his ransom.

f. When victims agreed to meet EPIFANIOU's ransom demand, EPIFANIOU demanded payment in bitcoin to his Blockchain.info bitcoin wallet or a wire of funds to a Bank of Cyprus bank account.

All in violation of Title 18, United States Code, Section 1349.

**COUNTS TWO THROUGH THREE**

(Wire Fraud)

5. The Grand Jury re-alleges and incorporates by reference paragraphs 2 through 4 of this Indictment as if fully set forth herein.

6. On or about the dates listed in Column B of the table below, in the Northern District of Georgia and elsewhere, the defendant, JOSHUA POLLOSO EPIFANIOU, a/k/a Charley Sullivan, a/k/a Chary Malatan, a/k/a Richard Charley, aided and abetted by others known and unknown to the Grand Jury, having knowingly devised and intended to devise the aforementioned scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises as set forth in Count One of this Indictment, did with intent to defraud cause the transmission by means of wire communication in interstate and foreign commerce of certain writings, signs, signals, pictures, and sounds, that is, bitcoin payments from Turner in the Northern District of Georgia in the amounts listed in Column C to the Blockchain.info wallet address listed in Column D owned by EPIFANIOU and maintained in Luxembourg, for the purpose of executing and attempting to execute such scheme and artifice:

| <b>A</b>     | <b>B</b>    | <b>C</b>      | <b>D</b>              |
|--------------|-------------|---------------|-----------------------|
| <b>Count</b> | <b>Date</b> | <b>Amount</b> | <b>Bitcoin Wallet</b> |
| <b>2</b>     | 11/16/2016  | 13.04 BTC     | Address ending Xn3K   |
| <b>3</b>     | 11/18/2016  | 12.80 BTC     | Address ending Xn3K   |

All in violation of Title 18, United States Code, Sections 1343 and 2.

**COUNT FOUR**

(Computer Fraud Conspiracy)

7. The Grand Jury re-alleges and incorporates by reference paragraphs 2 through 4 of this Indictment as if fully set forth herein.

8. Beginning on an unknown date, but at least by in or about October 2014, and continuing through in or about November 2016, in the Northern District of Georgia and elsewhere, the defendant, JOSHUA POLLOSO EPIFANIYOU, a/k/a Charley Sullivan, a/k/a Chary Malatan, a/k/a Richard Charley, did knowingly and intentionally combine, conspire, confederate, agree, and have a tacit understanding with other persons known and unknown to the Grand Jury, to:

- a. intentionally access a computer without authorization and exceeding authorization, and thereby obtain information from protected computers, the offense being committed for purposes of commercial advantage and private financial gain, and the value of the information obtained exceeding \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i), 1030(c)(2)(B)(iii); and
- b. knowingly transmit in interstate and foreign commerce a communication containing a threat to obtain information from a protected computer and to impair the confidentiality of information obtained from a protected computer, namely, personal identifying information obtained from customer and user databases, without

authorization and by exceeding authorized access, with intent to extort from any person any money and any other thing of value, in violation of Title 18, United States Code, Sections 1030(a)(7)(B).

**MANNER AND MEANS OF THE CONSPIRACY**

9. It was part of the conspiracy that the defendant, JOSHUA POLLOSO EPIFANIOU, a/k/a Charley Sullivan, a/k/a Chary Malatan, a/k/a Richard Charley, and others known and unknown employed the manner and means set forth in paragraph 4 of this Indictment to gain unauthorized access to the computer networks of U.S.-based websites, steal confidential personal identifying information from user and customer databases, and extort the victim companies into paying a ransom under the threat of public disclosure of the sensitive personal data, as set forth in paragraph 3 of this Indictment.

**OVERT ACTS**

10. In furtherance of the conspiracy, and in order to effect the purpose and objects thereof, the defendant, JOSHUA POLLOSO EPIFANIOU, a/k/a Charley Sullivan, a/k/a Chary Malatan, a/k/a Richard Charley, and others committed various overt acts in the Northern District of Georgia and elsewhere, including, but not limited to, the following:

a. Beginning on an unknown date, but at least by on or about October 26, 2014, EPIFANIOU gained unauthorized access to the computer networks of Armor Games by exploiting a security vulnerability on the public website. To provide proof of his unauthorized access, EPIFANIOU downloaded a directory



list of the Armor Games website into a text file and changed the administrator's email address.

b. On or about October 30, 2014, EPIFANIIOU again gained unauthorized access to the computer networks of Armor Games and downloaded user data from Armor Games's user database. EPIFANIIOU also removed database content to take the website offline, which prevented users from accessing the website.

c. On or about the same day, EPIFANIIOU, using the alias Richard Charley, sent an email to the chief executive officer ("CEO") of Armor Games demanding a ransom payment. EPIFANIIOU's email stated that if Armor Games paid him \$1,500 in bitcoin, he would provide a security audit and return "all the exploits, your files, and your database." The message threatened that if payment was not provided, then "malware [would be] hosted on the index page of your website and the whole user database and orders database, containing addresses, ip addresses, usernames, passwords, payment information, [and] email addresses will be leaked aka posted publicly." EPIFANIIOU claimed that he had user data for 450,000 users.

d. On or about the same day, EPIFANIIOU, using the alias Richard Charley, sent additional emails to Armor Games containing the CEO's date of birth, social security number, and residential address and stated "Let's see if you play your cards right or if you want to play games and piss me off."

e. On or about the same day, EPIFANIIOU sent another email to the Armor Games CEO in which he raised his ransom demand to \$1,650 "due to

conversion rates” and sent directions instructing Armor Games to create a bitcoin account. After Armor Games sent messages stating that “[w]e need our site back online today” and noting that keeping the site offline “will hurt our users,” EPIFANIIOU agreed to restore the site online after receipt of an initial payment of \$1,000 to a bitcoin wallet under his control.

f. On or about October 31, 2014, EPIFANIIOU restored the site online after receipt of the initial \$1,000 ransom payment from Armor Games via bitcoin. EPIFANIIOU demanded that Armor Games send the remaining \$650 payment to the same bitcoin wallet and stated that, once payment was received, “i leave you all alone ending it all with no damage done.”

g. On or about November 5, 2014, Armor Games sent an additional 1.92 bitcoin (\$650) to EPIFANIIOU’s bitcoin wallet based on his messages. In response, EPIFANIIOU explained that he gained unauthorized access to the website by a SQL injection, which is the insertion of malicious code into an entry field for remote command execution. EPIFANIIOU then demanded an additional bitcoin payment “[d]ue to the exchange rates and [bitcoin] being unstable,” and stated that “you never hear from me again.”

h. On or about the same day, Armor Games provided an additional payment of \$200 in bitcoin to the same bitcoin wallet under EPIFANIIOU’s control.

i. Beginning on an unknown date, but at least by on or about November 9, 2016, EPIFANIIOU received a portion of the Bleacher Report user database from an individual who gained unauthorized access to the Bleacher

Report website through a security vulnerability. The individual shared the stolen user database excerpt with EPIFANIOU through the Jabber instant messaging service.

j. On or about November 9, 2016, EPIFANIOU, using the alias Charley Sullivan, sent an email to the Bleacher Report chief technology officer (“CTO”) with the subject line “36 Hours” in which he falsely stated that he discovered and exploited a remote code execution vulnerability on the website. EPIFANIOU’s email demanded payment of a ransom within 36 hours and threatened that if payment were not provided, he would leak Bleacher Report’s full user database, which contained first and last names, usernames (email addresses), and password hash information, on a public website. EPIFANIOU requested that a total of \$19,000 in bitcoin be paid in two transactions. EPIFANIOU stated that after receiving the second payment, he would delete all of the exfiltrated user data, and Turner would not hear from him again.

k. On or about the same day, EPIFANIOU offered to pay a co-conspirator to send a text message to the Bleacher Report CTO about the ransom message. At EPIFANIOU’s request, the co-conspirator sent a text message to the CTO instructing him to check his email for “an urgent matter regarding bleacher.”

l. Over the next several days, Turner sent email messages to EPIFANIOU requesting that he provide evidence of the compromise. On or about November 12, 2016, EPIFANIOU sent records from Bleacher Report’s user database, which contained confidential personal identifying information of

Bleacher Report's users, and screenshots showing access to Bleacher Report's administrator panel.

m. Based on EPIFANIU's threats, Turner sent an initial payment of \$9,500 (13.037989 BTC) on or about November 16, 2016 to a bitcoin wallet address provided by EPIFANIU and the second payment of \$9,500 (12.804442 BTC) on or about November 18, 2016 to the same bitcoin wallet.

All in violation of Title 18, United States Code, Section 371.

**COUNT FIVE**

(Computer Fraud and Abuse)

11. The Grand Jury re-alleges and incorporates by reference paragraphs 2 through 4 and paragraphs 9 through 10 of this Indictment as if fully set forth herein.

12. On or about November 9, 2016 and continuing through on or about November 18, 2016, in the Northern District of Georgia and elsewhere, the defendant, JOSHUA POLLOSO EPIFANIU, a/k/a Charley Sullivan, a/k/a Chary Malatan, a/k/a Richard Charley, aided and abetted by others known and unknown to the Grand Jury, did knowingly transmit in interstate and foreign commerce a communication containing a threat to obtain information from a protected computer and to impair the confidentiality of information obtained from a protected computer, namely, personal identifying information obtained from Turner's user database, without authorization and by exceeding authorized access, with intent to extort from any person, namely Turner, any money and any other thing of value, in violation of Title 18, United States Code, Sections 1030(a)(7)(B) and 2.

**FORFEITURE PROVISION**

13. Upon conviction of one or more of the offenses alleged in Counts One through Three of this Indictment, the defendant, JOSHUA POLLOSO EPIFANIOU, a/k/a Charley Sullivan, a/k/a Chary Malatan, a/k/a Richard Charley, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), any and all property constituting, or derived from, proceeds obtained directly or indirectly as a result of said violations;

14. Upon conviction of one or more of the offenses alleged in Counts Four through Five of this Indictment, the defendant, JOSHUA POLLOSO EPIFANIOU, a/k/a Charley Sullivan, a/k/a Chary Malatan, a/k/a Richard Charley, shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), the defendant's interest in any and all personal property that was used or intended to be used to commit or to facilitate the commission of such violation, as well as any and all property constituting, or derived from, proceeds obtained directly or indirectly as a result of said violations; and

15. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

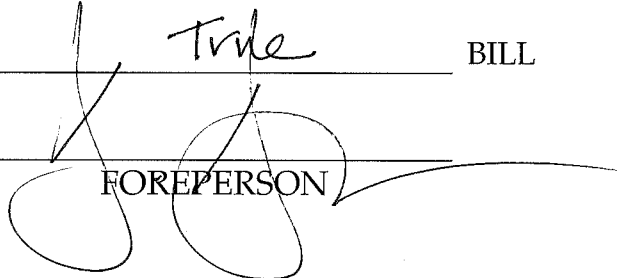
- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or

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

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b), to seek forfeiture of any other property of said defendant up to the value of the forfeitable property described above; all pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2)(A) & (B), and Title 28, United States Code, Section 2461(c).

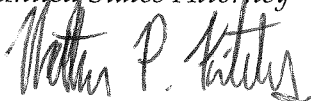
A True BILL

FOREPERSON



JOHN A. HORN

*United States Attorney*



NATHAN P. KITCHENS

*Assistant United States Attorney*

Georgia Bar No. 263930

600 U.S. Courthouse

75 Spring Street, S.W.

Atlanta, GA 30303

404-581-6000; Fax: 404-581-6181