IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

DIOGO SANTOS COELHO,
a/k/a "Omnipotent"
a/k/a "Downloading"
a/k/a "Shiza"
a/k/a "Kevin Maradona"

Defendant.

FILED UNDER SEAL

Case No. 1:21-cr-114

Count 1: Conspiracy to Commit Access Device Fraud
(18 U.S.C. § 1029(b)(2), § 3559(g)(l))

Count 2: Access Device Fraud — Using or Trafficking in an Unauthorized Access Device
(18 U.S.C. § 1029(a)(2) and 2)

Count 3: Access Device Fraud — Possession of Fifteen or More Unauthorized Access Devices
(18 U.S.C. § 1029(a)(3) and 2)

Counts 4-5: Access Device Fraud — Unauthorized Solicitation
(18 U.S.C. § 1029(a)(6) and 2)

Count 6: Aggravated Identity Theft
(18 U.S.C. § 1028A(a)(1) and 2)

Forfeiture Notice

SUPERSEDING INDICTMENT

February 2022 Term—at Alexandria, Virginia

THE GRAND JURY CHARGES THAT:

General Allegations

At all times material to this Indictment:

1. Defendant DIOGO SANTOS COELHO (a/k/a "Omnipotent," "Downloading," "Shiza," and "Kevin Maradona"), was a Portuguese national who resided in Portugal.

2. From at least in or around January 1, 2015 to on or about January 31, 2022, COELHO controlled and was the chief Administrator of a website www.Raidforums.com (the "RaidForums website"), which he operated with the help of other website Administrators. COELHO used the monikers "Omnipotent" and "Downloading" on the RaidForums website.

3. The RaidForums website was hosted on a server located outside the United States.

4. The RaidForums website served as a platform where members could solicit for sale, sell, and purchase contraband including, but not limited to, stolen access devices as defined in Title 18, United States Code, Section 1029(e)(1), means of identification as defined in Title 18, United States Code, Section 1028(d)(7), hacking tools, databases of hacked data, and other illegal services, such as hacking-for-hire.

5. An individual could access the RaidForums website without a membership. However, the website required an individual to sign up for a membership to solicit items for sale or purchase items. The RaidForums website offered four tiers of membership options, including in order of cost: (1) free membership; (2) VIP membership; (3) MVP membership; and (4) God membership. The more expensive the membership, the more access a user could get to the RaidForums website. The God membership, for example, offered almost unlimited access to the RaidForums website and features.

6. The RaidForums website sold "credits" to members, which granted members access to privileged areas of the website and enabled members to "unlock" and download stolen access devices, means of identification, and data from compromised databases, among other

items. Members could also earn credits through other means including, but not limited to, by posting instructions on how to commit certain illegal acts.

7. The RaidForums website had different forums where members could post about different subjects and offer items for sale. The forums included "Cracking," "Leaks," and "Marketplace," among others. The "Leaks" forum had a sub-forum entitled the "Leaks Market." The "Leaks Market" description stated that it was "[a] place to buy/sell/trade databases and leaks." The "Leaks Market" included for-sale listings for bank routing and account numbers, and stolen payment card data, such as payment card account numbers, card verification values ("CVV") or card verification codes ("CVC"), card expiration dates, or personal identification numbers. The "Leaks Market" sub-forum also displayed posts listing offers to sell the personal identifying information of individuals, such as names, email addresses, and social security numbers, and hacked databases of login credentials, such as usernames and associated passwords, for access to online accounts issued by United States entities.

8. COELHO offered an "Official Middleman Service" for a fee on the RaidForums website. More specifically, COELHO offered to accept cryptocurrency from the purchaser and files, including stolen access devices and means of identification, from the seller. COELHO then verified the contents of the files and conversed with the buyer and seller. Once the parties were satisfied, COELHO released the funds to the seller and the files, including stolen access devices and means of identification, to the purchaser.

COUNT 1

(*Conspiracy to Commit Access Device Fraud*)

THE GRAND JURY FURTHER CHARGES THAT:

9. The Grand Jury re-alleges and incorporates by reference the General Allegations of this Indictment.

10. Beginning from at least in or around June 2016 and continuing to on or about January 31, 2022, in an offense begun outside the jurisdiction of any particular State or district of the United States, and continued in the Eastern District of Virginia and elsewhere, the defendant, DIOGO SANTOS COELHO (a/k/a "Omnipotent," "Downloading," "Shiza," and "Kevin Maradona"), did knowingly and with the intent to defraud, combine, conspire, confederate, and agree with other persons both known and unknown to the Grand Jury, to commit and aid and abet the following offenses:

a. To knowingly and with the intent to defraud, traffic in and use one and more unauthorized access devices during a one-year period, to wit payment card data, bank routing and account numbers, social security numbers, and login credentials, including usernames and associated passwords, for access to online accounts provided by United States entities, and by such conduct obtain things of value aggregating $1,000 and more during that period, in violation of 18, United States Code, Sections 1029(a)(2);

b. To knowingly and with the intent to defraud, possess fifteen and more unauthorized access devices, to wit payment card data, bank routing and account numbers, social security numbers, and login credentials, including usernames and associated passwords, for access to online accounts issued by United States

entities, said conduct affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1029(a)(3); and

c. Without the authorization of the issuers of access devices, knowingly and with the intent to defraud, solicit individuals with the purpose of selling unauthorized access devices, to wit payment card data, bank routing and account numbers, social security numbers, and login credentials, including usernames and associated passwords, for access to online accounts issued by United States entities, said conduct affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1029(a)(6).

11. COELHO will be first brought to and arrested in the Eastern District of Virginia.

WAYS, MANNERS, AND MEANS

The primary purpose of the conspiracy was to make money through the trafficking in stolen access devices. The ways, manners, and means by which the defendant, DIOGO SANTOS COELHO, and his co-conspirators carried out the primary purpose of the conspiracy included, but were not limited to, the following:

12. It was part of the conspiracy that the defendant controlled and operated the RaidForums website.

13. It was further part of the conspiracy that the defendant operated the RaidForums website with the help of co-conspirators, who operated as Administrators of the RaidForums website. The defendant and other Administrators designed and administered the website's software and computer infrastructure; established and enforced website's rules; and created and managed sections of the website dedicated to promoting the buying and selling of contraband, including the "Leaks Market" sub-forum.

14. It was further part of the conspiracy that the defendant and his co-conspirators posted offers to sell stolen access devices on the RaidForums website, including, but not limited to, payment card data, bank routing and account numbers, social security numbers, and login credentials, including usernames and associated passwords, for access to online accounts issued by United States entities.

15. It was further part of the conspiracy that the defendant offered to sell "credits" to users, who could then use these "credits" to purchase stolen access devices on the RaidForums website, among other items.

16. It was further part of the conspiracy that the defendant offered a fee-based service, described as an "Official Middleman Service" on the RaidForums website, which enabled purchasers and sellers to verify the means of payment and contraband files being sold prior to executing the purchase and sale.

17. It was further part of the conspiracy that the defendant and his co-conspirators accepted payment in cryptocurrency in return for the sale of stolen access devices.

18. It was further part of the conspiracy that the defendant and his co-conspirators knowingly falsely registered a domain name, including RaidForums.com, and knowingly used that domain name in the course of committing the offense charged in Count 1, in violation 18 U.S.C. § 3559(g)(l).

OVERT ACTS

In furtherance of the conspiracy, and to effect the objects thereof, the defendant, DIOGO SANTOS COELHO, and his co-conspirators committed overt acts in the Eastern District of Virginia and elsewhere, including, but not limited to, the following:

19. On or about June 6, 2018, COELHO, using the moniker "Omnipotent," transferred the false registration of the domain "Raidforums.com" to a U.S.-based domain registrar based in Phoenix, Arizona using the alias "Kevin Maradona." COELHO falsely registered the domain name knowing that it was used to support the RaidForums website in furtherance of the conspiracy.

20. On or about July 24, 2018, COELHO, using the moniker "Omnipotent," made a posting on the RaidForums website, in which he advertised an "Official Middleman Service." The posting indicated that the service would enable both buyers and sellers to complete their transactions, and that COELHO would verify the contents of files to ensure buyers received the data that they expected to purchase.

21. On or about October 18, 2018, an unknown co-conspirator using the moniker "mariecurie" made a posting on the RaidForums website, which offered for sale stolen access devices, to wit, usernames and associated passwords for access to user accounts issued by an electronic commerce company in the United States ("Company 1").

22. On or about October 22, 2018, in the Eastern District of Virginia and elsewhere, an undercover law enforcement officer used eight credits, which the officer purchased on the RaidForums website, to "unlock" and download the Company 1 usernames and associated passwords that user "mariecurie" offered for purchase.

23. On or about December 16, 2018, COELHO, who was using the moniker "Downloading," made a posting on the RaidForums website, which offered for sale 2.3 million payment card account numbers, including the names, addresses, and phone numbers associated with the payment card account numbers, which were purportedly obtained from a breach of records belonging to United States hotels.

24. On or about February 5, 2019, in the Eastern District of Virginia and elsewhere, COELHO, who was using the moniker "Downloading," informed an undercover law enforcement officer that the stolen payment card data described in paragraph 23 were still available for sale.

25. On or about March 4, 2019, in the Eastern District of Virginia and elsewhere, COELHO, who was using the moniker "Downloading," provided an undercover law enforcement officer with three stolen access devices, to wit, payment card account numbers, card verification values, expiration dates, and the names associated with the payment cards. COELHO agreed to this exchange to convince the undercover law enforcement officer that "Downloading" could be trusted to sell approximately 1.1 million stolen access devices in exchange for a Bitcoin amount that was equivalent to approximately $4,000 at the time.

26. On or about March 5, 2019, in the Eastern District of Virginia and elsewhere, COELHO, who was using the monikers "Downloading," "Omnipotent," and "Shiza," arranged to both sell and serve as the middleman in the transaction to sell approximately 1.1 million stolen access devices to the undercover law enforcement officer. COELHO received a Bitcoin amount that was then equivalent to approximately $4,000; however, he did not provide the stolen access devices.

27. On or about April 5, 2020, an unknown co-conspirator using the moniker "fairbanksfires" made a posting on the RaidForums website, which offered for sale stolen access devices associated with an online tax filing company in the United States. The stolen access devices included, but were not limited to, social security numbers, email addresses, passwords, and bank routing and account numbers.

28. On or about April 25, 2020, COELHO, who was using the moniker "Omnipotent," executed his middleman service and aided and abetted "fairbanksfires" in selling stolen access devices to a confidential human source ("CHS"), who was working with the Federal Bureau of Investigation. The CHS transferred a Bitcoin amount that was then equivalent to approximately $4,000 to COELHO in furtherance of this transaction. COELHO then provided the CHS with a link, which enabled the CHS to download the stolen access devices.

29. On or about April 27, 2020, the CHS communicated to COELHO that the funds could be released to "fairbanksfires."

30. From on or about October 26, 2016 until at least on or about July 24, 2020, the RaidForums website offered for sale in its Official Database Index a 2015 database, which included stolen access devices, namely associated email addresses, passwords, names, and addresses for gaining access to online customer accounts issued by a major broadcasting and cable company in the United States ("Company 2").

31. On or about July 24, 2020, in the Northern District of Illinois and elsewhere, an undercover law enforcement officer used eight credits, which the officer purchased on the RaidForums website, to "unlock" and download the Company 2 database, as described in paragraph 30.

32. On or about August 11, 2021, a known individual using the moniker "SubVirt" posted on the RaidForums website an offer to sell recently hacked data with the following title: "SELLING-124M-U-S-A-SSN-DOB-DL-database-freshly-breached." This post provided a small sample of data, which included names and dates of birth, and priced the information at six (6) Bitcoin.

33. On or about August 14, 2021, a known individual using the moniker "SubVirt" created a revised post on the RaidForums website offering to sell recently hacked data with the following title: "SELLING 30M SSN + DL + DOB database." This post provided a small sample of data, which included names and dates of birth, and priced the information at six (6) Bitcoin. The post also provided a Telegram handle as contact information for interested buyers. A subsequent post confirmed that the hacked data belonged to a major telecommunications company and wireless network operator that provides services in the United States ("Company 3").

34. On or about August 17, 2021, COELHO, who was using the moniker "Omnipotent," executed his middleman service and aided and abetted "SubVirt" in selling a sample of confidential and sensitive information and other data of value obtained during an unlawful computer intrusion, including, but not limited to, customer names, social security numbers, dates of birth, driver's license numbers, phone numbers, billing account numbers, customer relationship manager information, Mobile Station Integrated Services Digital Network (MSISDN) information, International Mobile Subscriber Identity (IMSI) numbers, and International Mobile Equipment Identity (IMEI) numbers to a third-party then operating on behalf of Company 3. The third-party used COELHO's middleman service to transfer a Bitcoin amount that was then equivalent to approximately $50,000 to "SubVirt."

35. On or about August 22, 2021, COELHO, who was using the moniker "Omnipotent," executed his middleman service and aided and abetted "SubVirt" in selling complete database sets containing confidential and sensitive information and other data of value obtained during an unlawful computer intrusion, including, but not limited to, customer names, social security numbers, dates of birth, driver's license numbers, phone numbers, billing account

numbers, customer relationship manager information, MSISDN information, IMSI numbers, and IMEI numbers to a third-party then operating on behalf of Company 3. The third-party used COELHO's middleman service to transfer a Bitcoin amount that was then equivalent to approximately $150,000 to "SubVirt."

(All in violation of Title 18, United States Code, Sections 1029(b)(2) and 3559(g)(1))

COUNT 2

(*Access Device Fraud — Using or Trafficking in an Unauthorized Access Device*)

THE GRAND JURY FURTHER CHARGES THAT:

36. The factual allegations in paragraphs 1 through 8 and 23 to 26 are re-alleged and incorporated as if fully set forth below.

37. From on or about February 5, 2019 until on or about March 5, 2019, in the Eastern District of Virginia and elsewhere, the defendant, DIOGO SANTOS COELHO (a/k/a "Omnipotent," "Downloading," "Shiza," and "Kevin Maradona"), knowingly and with the intent to defraud, did traffic in and use one and more unauthorized access devices, to wit, payment card account numbers, card verification values, expiration dates, and other associated information, during a one-year period, to wit, from January 1, 2019, through December 31, 2019, and by such conduct did obtain things of value aggregating $1,000 and more during that period, to wit, the Bitcoin worth approximately $4,000 on or about March 5, 2019, said trafficking affecting interstate and foreign commerce, in that the trafficking occurred via the Internet, and between computers located inside the Commonwealth of Virginia, and computers located outside of the Commonwealth of Virginia.

(In violation of Title 18, United States Code, Section 1029(a)(2) and 2)

COUNT 3

(*Access Device Fraud — Possession of Fifteen or More Unauthorized Access Devices*)

THE GRAND JURY FURTHER CHARGES THAT:

38. The factual allegations in paragraphs 1 through 8 and 30 to 31, are re-alleged and incorporated as if fully set forth below.

39. From on or about October 26, 2016 until on or about July 24, 2020, within the jurisdiction of the United States and in an offense begun and committed outside the jurisdiction of a particular State or district, including in Portugal, Germany, and elsewhere, the defendant, DIOGO SANTOS COELHO (a/k/a "Omnipotent," "Downloading," "Shiza," and "Kevin Maradona"), did knowingly and with intent to defraud, possess fifteen or more unauthorized access devices as defined by 18 U.S.C. § 1029(e)(2), and (e)(3), to wit, email addresses, associated passwords, and other related information to access the customer accounts of subscribers to a major broadcasting and cable company in the United States, said possession affecting interstate and foreign commerce.

40. COELHO will be first brought to and arrested in the Eastern District of Virginia.

(In violation of Title 18, United States Code, Section 1029(a)(3) and 2)

COUNTS 4-5

(*Access Device Fraud —Unauthorized Solicitation*)

THE GRAND JURY FURTHER CHARGES THAT:

41. The factual allegations in paragraphs 1 through 8 and 21 through 26 are re-alleged and incorporated as if fully set forth below.

42. On or about the dates identified below, in the Eastern District of Virginia and elsewhere, the defendant, DIOGO SANTOS COELHO (a/k/a "Omnipotent," "Downloading," "Shiza," and "Kevin Maradona"), did knowingly and with intent to defraud solicit other persons for the purpose of offering unauthorized access devices as defined by 18 U.S.C. § 1029(e)(2), and (e)(3), to wit, the access devices as set forth below in each count, without the authorization of the issuer of the access devices, said solicitation affecting interstate and foreign commerce, in that the solicitation occurred via the Internet, and between computers located inside the Commonwealth of Virginia, and computers located outside of the Commonwealth of Virginia.

Count	Date	Description of Access Device
4	October 18 to 22, 2018	Usernames and passwords for access to online accounts issued by an electronic commerce company in the United States
5	December 16, 2018 to March 5, 2019	Payment card account numbers, card verification values, and expiration dates

(In violation of Title 18, United States Code, Section 1029(a)(6) and 2)

COUNT 6

(*Aggravated Identity Theft*)

THE GRAND JURY FURTHER CHARGES THAT:

43. The factual allegations in paragraphs 1 through 8 and 23 through 26 are re-alleged and incorporated as if fully set forth below.

44. From on or about December 16, 2018 until on or about March 5, 2019, in an offense begun outside the jurisdiction of any particular State or district of the United States, and continued in the Eastern District of Virginia and elsewhere, the defendant, DIOGO SANTOS COELHO (a/k/a "Omnipotent," "Downloading," "Shiza," and "Kevin Maradona"), did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit, access device fraud, in violation of 18 U.S.C. §§ 1029(a)(2) and (a)(6) as alleged in Counts 2 and 5 of this Indictment, knowing that the means of identification belonged to another actual person.

45. COELHO will be first brought to and arrested in the Eastern District of Virginia.

(In violation of Title 18, United States Code, Section 1028A(a)(1) and 2)

FORFEITURE NOTICE

THE GRAND JURY HEREBY FINDS THAT:

46. There is probable cause that the property described in this NOTICE OF FORFEITURE is subject to forfeiture pursuant to the statutes described herein.

47. The defendant is hereby notified, pursuant to Fed.R.Crim.P. 32(a), that upon conviction of the offenses set forth in Counts 1-5 of this Indictment, the defendant, DIOGO SANTOS COELHO, shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 982(a)(2)(B) any property constituting, or derived from, proceeds the defendant obtained directly or indirectly, as the result of such violation; and pursuant to Title 18, United States Code, Section 1029(c)(1)(C), any personal property used or intended to be used to commit the offenses. The assets subject to forfeiture include, but are not limited to, the following:

a. The domain name RaidForums.com;

b. The domain name raid.lol;

c. The domain name rf.ws;

d. One Samsung smartphone model SM-G950F;

e. One Lenovo tablet with serial number HGER85N8;

f. One Acer laptop with serial number NXGNLEB00272108E6B7200;

g. One Yubico authentication device;

h. One Sony Digital Camera with serial number 4098514; and

i. A money judgment in the amount of not less than $215,571, representing the proceeds the defendant obtained as a result of the violations described in this Indictment.

48. Pursuant to 21 U.S.C. § 853(p), the defendant shall forfeit substitute property, if, by any act or omission of the defendant, the property referenced above cannot be located upon the exercise of due diligence; has been transferred, sold to, or deposited with a third party; has been placed beyond the jurisdiction of the Court; has been substantially diminished in value; or has been commingled with other property which cannot be divided without difficulty.

(All in accordance with Title 18, United States Code, Section 982(a)(2)(B), Title 18, United States Code, Section 1029(c)(1)(C), and Federal Rule of Criminal Procedure 32.2).

A TRUE BILL

FOREPERSON

Jessica D. Aber
United States Attorney

By: _____
Carina A. Cuellar
Assistant United States Attorney

Aarash A. Haghighat
Senior Counsel
Computer Crime and Intellectual Property Section
United States Department of Justice