UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

UNITED STATES OF AMERICA

v.

CASE NO. 8:20-cr-238-T-30SPF

18 U.S.C. § 371
18 U.S.C. § 1349
18 U.S.C. § 1956(h)
18 U.S.C. § 1029(a)(3)
18 U.S.C. § 1029(a)(6)(A)
18 U.S.C. § 1030(a)(2)(C)

SANDU BORIS DIACONU,
a/k/a "utmsandu"
a/k/a "sandushell"
a/k/a "rootarhive"
a/k/a "WinD3str0y," and
[redacted]

INDICTMENT

The Grand Jury charges:

COUNT ONE
(Conspiracy to Commit Access Device Fraud, to Access a Protected Computer, and to Access a Protected Computer in Furtherance of Fraud)

A. Introduction

At times material to this Indictment:

1. SANDU BORIS DIACONU ("DIACONU"), a/k/a "utmsandu," a/k/a "sandushell," a/k/a "rootarhive," a/k/a "WinD3str0y," was a citizen of Moldova who resided in that country.

2. [redacted]

3. DIACONU and [redacted] were both administrators of a publicly accessible website that was comprised of several domains (hereinafter, the "Marketplace"). DIACONU and [redacted] developed, commissioned the development of, administered, and used the Marketplace.

4. The Marketplace was an e-commerce storefront that facilitated the unauthorized sale of login credentials (i.e., usernames and passwords) for compromised computers and servers (hereinafter, "compromised servers") located around the world. This included the unauthorized sale of credentials and servers belonging to United States citizens, including servers, entities, and individuals located in the Middle District of Florida.

5. There was no legitimate business conducted on the Marketplace. The Marketplace existed solely as a platform for individuals to buy and sell access to compromised servers.

6. Victim-1 was a business entity located in Maitland, Florida.

7. Victim-2 was a religious congregation located in Tampa, Florida.

8. Victim-3 was a medical practice and a business entity located in Tampa, Florida.

9. Victim-4 was a business entity located in Tampa, Florida.

10. Victim-5 was a business entity located in Tampa, Florida.

11. Victim-6 was a local public agency located in Tampa, Florida.

12. Victim-7 was a business entity located in Orlando, Florida.

Definitions

13. A "server" was a computer that provided services for other computers connected to it via a computer network (i.e., a set of computers connected together locally for the purpose of sharing resources) or the internet. Servers could be physically located and accessed anywhere with a network or internet connection. A server could have been either a physical or virtual machine.

14. An "internet protocol address" or "IP address" was a unique identifier assigned to every computer on the internet or a local network, much like a phone number. An IP address could at times be used to identify the location of the computer connected to the internet.

15. "Remote Desktop Protocol" or "RDP" was a proprietary protocol developed by Microsoft that allowed a user to connect to another computer over a network and control the computer remotely. When used legitimately, RDP allowed a user to access his or her computer remotely, such as an employee working on the employer's network from the employee's home. When used without authorization, RDP could allow a cybercriminal to compromise and take control of a victim's computer and server network.

16. "Secure Shell," "Secure Socket Shell," or "SSH" was a network protocol that allowed a user to securely access a computer remotely over an unsecured network. The protocol worked in the client-server model, which meant that the connection was established by the SSH client connected to the SSH server. The SSH client used public key cryptography to verify the identity of the SSH server. The SSH protocol used encryption and hashing algorithms to provide privacy and integrity of the data that was exchanged between the client and server.

17. Digital currencies were electronically sourced units of value that existed on the internet and were not stored in a physical form, nor were they issued by any government.

18. "Bitcoin" was a type of digital currency. Bitcoin was generated and controlled through computer software operating on decentralized peer-to-peer (or person-to-person) networks. Users of Bitcoin sent units of value to and from "addresses," which were unique strings of numbers and letters that functioned like a bank account number. Bitcoin transactions were recorded on a publicly available, distributed ledger, known as a "blockchain." Because Bitcoin was transferred peer-to-peer, users could avoid traditional, regulated financial institutions that collected information about their customers and maintained anti-money laundering and bank secrecy programs.

19. "Perfect Money" was a service that allowed users to make online payments and financial transfers. Users of Perfect Money could easily deposit Bitcoin, United States dollars, and other currency into a Perfect Money account. Once deposited, users of Perfect Money could utilize these funds to pay for goods and services online. Perfect Money could also be utilized by a user to accept payments on behalf of his or her internet-based business.

20. An "access device" was any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that could be used alone or in conjunction with another access device to obtain money, goods, services, or any other thing of value, or that could be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

21. An "unauthorized access device" was any access device that was lost, stolen, expired, revoked, canceled, or obtained with intent to defraud.

The Marketplace

22. The Marketplace existed primarily as a place for individuals to buy and sell RDP and SSH access (login credentials) to compromised servers, which was used to facilitate a wide range of illegal activity, such as

ransomware attacks, fraudulent wire transfers, and tax fraud.

23. The Marketplace looked like a traditional e-commerce website and functioned like a legitimate business would. The Marketplace touted the fact that it sold valid login credentials to compromised servers, offered an exchange and warranty policy, and offered high-quality customer service.

24. The Marketplace was written in English and its homepage allowed users ("buyers") to view their account balances, view available RDP and SSH access, view their purchases, change account settings, and communicate via web-based email.

25. The Marketplace provided a search tool that allowed buyers to search for login credentials of compromised servers based on a variety of criteria, including: the country, region or zip code of the compromised server; the operating system of the compromised server; the internet service provider of the compromised server; the purchase price of the credentials; and, whether the compromised server had certain open ports.

26. The Marketplace also provided numerous avenues for customer support, including explanatory pages, "Support" and "Contacts" pages, and terms and conditions. DIACONU's contact information was listed for some of these customer support functions.

27. Perfect Money was used for all purchases on the Marketplace. The Marketplace also operated and advertised a sister website that allowed buyers to convert Bitcoin into Perfect Money.

28. Before purchasing login credentials to a compromised server, a buyer would load Perfect Money funds onto their account on the Marketplace. The Marketplace did not allow for transactions in official, government-backed currencies (such as United States dollars), which made it harder for government agencies to detect and track illicit transactions.

B. The Conspiracy

29. Beginning on an unknown date, but at least as early as on or about January 22, 2015, and continuing until at least on or about February 27, 2020, in the Middle District of Florida and elsewhere, the defendants,

SANDU BORIS DIACONU,
a/k/a "utmsandu,"
a/k/a "sandushell,"
a/k/a "rootarhive,"
a/k/a "WinD3str0y," and
[redacted]

did knowingly and willfully combine, conspire, and agree with each other and with other persons, known and unknown to the Grand Jury, to commit offenses against the United States, that is:

a. Possession of fifteen or more unauthorized access devices, in violation of 18 U.S.C. § 1029(a)(3);

b. Unauthorized solicitation of an access device, in violation of 18 U.S.C. § 1029(a)(6)(A); and

c. Obtaining information by computer from a protected computer, in furtherance of another criminal violation, in violation of 18 U.S.C. § 1030(a)(2)(C).

C. Manner and Means

30. The manner and means by which the conspirators sought to accomplish the objects of the conspiracy included, among others:

a. It was part of the conspiracy that conspirators would and did develop, and commission the development of, the Marketplace so as to, among other things, assist sellers (including themselves) in offering login credentials for compromised servers around the world, assist buyers in perpetrating fraud using those login credentials, and enrich themselves and others;

b. It was a further part of the conspiracy that conspirators would and did operate administrator accounts to maintain and oversee the Marketplace;

c. It was a further part of the conspiracy that conspirators would and did offer contact information and customer support services to buyers on the Marketplace;

d. It was a further part of the conspiracy that conspirators would and did use wire transmissions, including emails, electronic data transfers, and web-based communications, as well as other instrumentalities of interstate and foreign commerce, to facilitate their operation and administration of the Marketplace;

e. It was a further part of the conspiracy that conspirators would and did employ various techniques to protect their anonymity and to thwart detection of their activities by government and law-enforcement agencies;

f. It was a further part of the conspiracy that conspirators would and did cultivate and use online monikers that were distinct from their true identities;

g. It was a further part of the conspiracy that conspirators would and did advertise the Marketplace, so as to promote the Marketplace and to attract new buyers;

h. It was a further part of the conspiracy that conspirators would and did require the Marketplace buyers to use Perfect Money to make

purchases on the Marketplace, so as to conceal the identities of conspirators and other buyers, as well as to conceal the illicit activity that was occurring on the Marketplace;

i. It was a further part of the conspiracy that conspirators would and did operate a sister website that allowed buyers to convert Bitcoin into Perfect Money;

j. It was a further part of the conspiracy that conspirators would and did advertise the sister website that allowed buyers to convert Bitcoin into Perfect Money, including by listing a link to the website on the main sidebar of the Marketplace and offering a discount for buyers to use the conversion service;

k. It was a further part of the conspiracy that the Marketplace administrator conspirators would and did create and maintain records for buyers, including usernames, registration dates, email addresses, purchases, Perfect Money balances, last login dates, and the IP address of buyers at the time of last login;

l. It was a further part of the conspiracy that conspirators would and did create listings for compromised servers, which listings included the country, region or zip code of the compromised server, the operating system of the compromised server, the internet service provider of the

compromised server; the purchase price of the credentials, and whether the compromised server had certain open ports;

m. It was a further part of the conspiracy that conspirators would and did create listings for login credentials for compromised servers throughout the United States, including compromised servers located in the Middle District of Florida;

n. It was a further part of the conspiracy that conspirators would and did share in the proceeds that the Marketplace generated, so as to promote and perpetuate the scheme, as well as to enrich themselves; and

o. It was further part of the conspiracy that conspirators would and did perform acts and make statements to misrepresent, hide, and conceal, and cause to be misrepresented, hidden, and concealed, the purpose of the conspiracy and the acts committed in furtherance thereof.

D. Overt Acts

31. In furtherance of the conspiracy, and to effect the objects thereof, the following overt acts, among others, were committed in the Middle District of Florida and elsewhere:

a. On or about January 22, 2015, conspirators created the Marketplace;

b. On or about January 22, 2015, DIACONU registered an administrator account with the Marketplace;

c. On or about December 7, 2016, [redacted] registered for services to host the Marketplace and the sister website's code and database;

d. On or about December 10, 2016, DIACONU registered the moniker "WinD3str0y" for his administrator account;

e. On or about December 18, 2016, [redacted] registered an administrator account with the Marketplace;

f. On an unknown date, .zip files were created within subfolders on the Marketplace that listed a user name associated with [redacted]

g. On January 18, 2017, DIACONU received a buyer's email regarding non-working RDP access and requesting a refund;

h. On or about February 5, 2017, conspirators facilitated the sale of login credentials for Victim-1's server;

i. On or about August 17, 2018, [redacted] registered a new domain for the Marketplace with a domain name registrar;

j. On or about August 17, 2018, DIACONU made a payment to the domain name registrar for the Marketplace's domain;

k. On or about August 19, 2018, [redacted]ent a test message from the Marketplace's domain to his email account;

l. On or about August 26, 2018, DIACONU sent an email to approximately 30 individuals addressing the transitioning of the Marketplace to a new domain;

m. On or about January 3, 2019, a conspirator exchanged customer support messages with an undercover agent posing as a buyer of RDP access for servers located in the Middle District of Florida;

n. On or about January 8, 2019, conspirators facilitated the sale of login credentials for Victim-7's server;

o. On or about March 19, 2019, DIACONU logged into the Marketplace using his administrator account;

p. On or about May 29, 2019, [redacted]ntentionally accessed Victim-2's server without authorization;

q. On or about July 23, 2019, conspirators facilitated the sale of login credentials for Victim-3's server;

r. On or about July 23, 2019, conspirators facilitated the sale of login credentials for Victim-4's server;

s. On or about August 14, 2019, conspirators facilitated the sale of login credentials for Victim-5's server; and

t. On or about August 15, 2019, conspirators facilitated the sale of login credentials for Victim-6's server.

All in violation of 18 U.S.C. § 371.

COUNT TWO
(Conspiracy to Commit Wire Fraud)

A. Introduction

1. Paragraphs 1 through 28 of Count One of this Indictment are hereby realleged and incorporated by reference as though fully set forth herein.

B. The Conspiracy

2. Beginning on an unknown date, but at least as early as on or about January 22, 2015, and continuing until at least the present date, in the Middle District of Florida and elsewhere, the defendants,

SANDU BORIS DIACONU,
a/k/a "utmsandu,"
a/k/a "sandushell,"
a/k/a "rootarhive,"
a/k/a "WinD3str0y," and
[redacted]

did knowingly and willfully combine, conspire, and agree with each other and with other persons, both known and unknown to the Grand Jury, to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises that

related to material facts, and, for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, any writings, signs, signals, pictures, and sounds, in violation of 18 U.S.C. § 1343.

C. Manner and Means

3. Paragraphs 30(a)-(o) of Count One of this Indictment are hereby realleged and incorporated by reference as though fully set forth herein.

All in violation of 18 U.S.C. § 1349.

COUNT THREE
(Conspiracy to Commit Money Laundering)

A. Introduction

1. Paragraphs 1 through 28 of Count One of this Indictment are hereby realleged and incorporated by reference as though fully set forth herein.

B. The Conspiracy

2. Beginning on an unknown date, but at least as early as on or about January 22, 2015, and continuing until at least on or about February 27, 2020, in the Middle District of Florida and elsewhere, the defendants,

SANDU BORIS DIACONU,
a/k/a "utmsandu,"
a/k/a "sandushell,"
a/k/a "rootarhive,"
a/k/a "WinD3str0y," and
[redacted]

[redacted]

did knowingly and willfully combine, conspire, and agree with each other and with other persons, both known and unknown to the Grand Jury, to commit an offense, that is, to conduct a financial transaction affecting interstate and foreign commerce, namely, to transport, transmit, and transfer monetary instruments and funds which involved the proceeds of a specified unlawful activity, that is, wire fraud, in violation of 18 U.S.C. § 1343, knowing that the transaction was designed in whole and in part to conceal and disguise the nature, location, source, ownership and control of the proceeds of said specified unlawful activity, knowing that the property involved in the financial transaction represented the proceeds of some form of unlawful activity, in violation of 18 U.S.C. § 1956(a)(1)(B)(i).

C. Manner and Means

3. Paragraphs 30(a)-(o) of Count One of this Indictment are hereby realleged and incorporated by reference as though fully set forth herein.

All in violation of 18 U.S.C. § 1956(h).

COUNT FOUR
(Possession of Fifteen or More Unauthorized Access Devices)

A. Introduction

1. Paragraphs 1 through 28 of Count One of this Indictment are hereby realleged and incorporated by reference as though fully set forth herein.

B. The Offense

2. On or about January 17, 2017, in the Middle District of Florida and elsewhere, the defendants,

SANDU BORIS DIACONU,
a/k/a "utmsandu,"
a/k/a "sandushell,"
a/k/a "rootarhive,"
a/k/a "WinD3str0y," and
[redacted]

aided and abetted by each other and by other persons, known and unknown to the Grand Jury, did knowingly and with intent to defraud possess 15 or more unauthorized access devices, that is, credentials to access 15 or more compromised servers located in the Middle District of Florida, said possession affecting interstate and foreign commerce.

In violation of 18 U.S.C. §§ 1029(a)(3) and 2.

COUNT FIVE
(Unauthorized Solicitation of an Access Device)

A. Introduction

1. Paragraphs 1 through 28 of Count One of this Indictment are hereby realleged and incorporated by reference as though fully set forth herein.

B. The Offense

2. On or about February 5, 2017, in the Middle District of Florida and elsewhere, the defendants,

SANDU BORIS DIACONU,
a/k/a "utmsandu,"
a/k/a "sandushell,"
a/k/a "rootarhive,"
a/k/a "WinD3str0y," and
[redacted]

aided and abetted by each other and by other persons, known and unknown to the Grand Jury, did knowingly and with intent to defraud, and without the authorization of the issuer of the access device, that is, Victim-1, located in the Middle District of Florida, solicit a person for the purpose of offering an access device, that is, credentials to a compromised server belonging to Victim-1, said conduct affecting interstate and foreign commerce.

In violation of 18 U.S.C. §§ 1029(a)(6)(A) and 2.

COUNT SIX
(Obtaining Information by Computer from a Protected Computer)

A. Introduction

1. Paragraphs 1 through 28 of Count One of this Indictment are hereby realleged and incorporated by reference as though fully set forth herein.

B. The Offense

2. On or about May 29, 2019, in the Middle District of Florida and elsewhere, the defendants,

SANDU BORIS DIACONU,
a/k/a "utmsandu,"
a/k/a "sandushell,"
a/k/a "rootarhive,"
a/k/a "WinD3str0y," and
[redacted]

aided and abetted by each other and by other persons, known and unknown to the Grand Jury, did intentionally access a computer without authorization, that is, a computer belonging to Victim-2, located in Tampa, Florida, and thereby obtained information from a protected computer, in furtherance of a criminal violation of the laws of the United States, that is, a violation of 18 U.S.C. § 1349.

In violation of 18 U.S.C. §§ 1030(a)(2)(C) and 2.

FORFEITURE

1. The allegations contained in this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to the provisions of 18 U.S.C. §§ 981(a)(1), 982(a)(1), 982(a)(2), 1029(c)(1)(C), 1030(i), and 28 U.S.C. § 2461(c).

2. Upon conviction of a violation of 18 U.S.C. § 1029, or a conspiracy to violate 18 U.S.C. § 1029 (18 U.S.C. § 371), the defendants,

SANDU BORIS DIACONU,
a/k/a "utmsandu,"
a/k/a "sandushell,"
a/k/a "rootarhive,"
a/k/a "WinD3str0y," and
[redacted]

shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(2)(B), any property constituting, or derived from, proceeds the person obtained directly or indirectly, as a result of such violation, and pursuant to 18 U.S.C. § 1029(c)(1)(C), any personal property used or intended to be used to commit the offense.

3. Upon conviction of a violation of 18 U.S.C. § 1030, or a conspiracy to violate 18 U.S.C. § 1030 (18 U.S.C. § 371), the defendants,

SANDU BORIS DIACONU,
a/k/a "utmsandu,"
a/k/a "sandushell,"
a/k/a "rootarhive,"
a/k/a "WinD3str0y," and
[redacted]

shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(2)(B), any property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of such violation and, pursuant to 18 U.S.C. § 1030(i), any personal property used or intended to be used to commit or to facilitate the commission of such violation.

4. Upon conviction of a conspiracy of the violation of 18 U.S.C. § 1343, in violation of 18 U.S.C. § 1349, the defendants,

SANDU BORIS DIACONU,
a/k/a "utmsandu,"
a/k/a "sandushell,"
a/k/a "rootarhive,"
a/k/a "WinD3str0y," and
[redacted]

shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the offense.

5. Upon conviction of a violation of 18 U.S.C. § 1956(h), the defendants,

SANDU BORIS DIACONU,
a/k/a "utmsandu,"
a/k/a "sandushell,"
a/k/a "rootarhive,"
a/k/a "WinD3str0y," and
[redacted]

shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(1), any property, real or personal, involved in such offense, or any property traceable to such property.

6. If any of the forfeitable assets described above, as a result of any act or omission of the defendants:

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third person;

(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 subdivided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property under the provisions of 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. § 982(b)(1) and 28 U.S.C. § 2461(c).

A TRUE BILL,

[redacted]

Foreperson

MARIA CHAPA LOPEZ
United States Attorney

By: _____
Patrick D. Scruggs
Assistant United States Attorney

By: _____
Rachel K. Jones
Assistant United States Attorney

By: _____
Cherie L. Krigsman
Assistant United States Attorney
Chief, National Security and Cybercrime Section

FORM OBD-34
August 20

No.

UNITED STATES DISTRICT COURT
Middle District of Florida
Tampa Division

THE UNITED STATES OF AMERICA

vs.

SANDU BORIS DIACONU,
a/k/a "utmsandu", a/k/a "sandushell", a/k/a "rootarhive" a/k/a "WinD3str0y" and

[redacted]

INDICTMENT

Violations: 18 U.S.C. § 371, 18 U.S.C. § 1349,
18 U.S.C. § 1956(h), 18 U.S.C. § 1029(a)(3),
18 U.S.C. § 1029(a)(6)(A), 18 U.S.C. § 1030(a)(2)(C)

A true bill,

[redacted]

Foreperson

Filed in open court this 11th day

AUG 2020

CLERK, US DISTRICT COURT
MIDDLE DISTRICT FLORIDA
TAMPA, FLORIDA

Clerk

2020 AUG 11 PM 2:02

Bail $ FILED