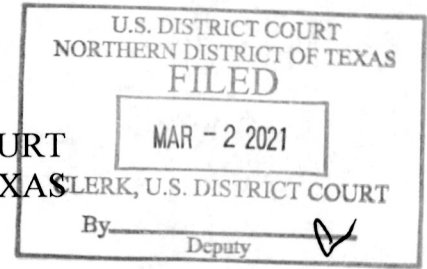


ORIGINAL

SEALED

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION



UNITED STATES OF AMERICA

v.

SORIN BECHERU

a.k.a. t0r.creep.im

a.k.a. turan1@jabbim.com

a.k.a. buchetta@jabb3r.de

3-21 CR0098 - X

CRIMINAL NO.

FILED UNDER SEAL

INDICTMENT

The Grand Jury charges:

At all times material to this Indictment:

Introduction

1. The “deep web” is the portion of the Internet not indexed by search engines, such as internal networks belonging to private industry, government agencies, or academic institutions.

2. The “dark web” is a portion of the deep web that has been intentionally hidden and is inaccessible through standard web browsers.

3. To access the dark web, individuals must use specialized software to access content and websites. Within the dark web, criminal marketplaces operate, allowing individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes

called the “clear web” or simply the “web”). These online market websites use a variety of encryption technologies to ensure that communications and transactions are shielded from interception and monitoring, and operate similarly to clear web commercial websites such as Amazon or eBay, but offer illicit goods and services.

4. An “online carding forum” is an illegal site dedicated to the sharing of stolen credit card information. A carding forum may include credit card information that has been illegally obtained, as well as a discussion boards in which members of the forum may share techniques used in obtaining credit card information. Online carding forums have buyers, sellers, and administrators of the site. Administrators help run and facilitate the distribution of illegally obtained credit card information.

5. Victim credit card information found on online carding forums generally includes the actual credit card number, cardholder name, expiration date and security code on the back as well as the billing address and phone number. Sellers on online carding forums will sell credit card information in batches. These batches can be categorized by location and timing of when the credit card information was illegally acquired.

6. Sellers will acquire victim credit card information using various tactics to include: key logging, phishing, vulnerability exploitation, and “Point of Sale” (POS) memory scraping malware.

7. “POS terminals” are the main processing devices between the buyer and seller when a card based payment system is involved. “POS memory scraping malware” is a special purpose malware program that is designed to scrape data from the terminal’s main memory. The malware will steal the unencrypted data that gets copied to the terminal’s

primary memory (RAM) when a credit or debit card is supplied to it for payment processing. This data is then exfiltrated to a server controlled by the Seller. The Seller is then able to take this data and sell it in online carding forums on the dark web for payment, generally through cryptocurrency.

8. After purchasing the victim credit card information on the dark web, buyers can then use the victim credit card information to purchase goods and services from retailers online or in person in the Northern District of Texas and elsewhere.

9. Sorin Becheru is citizen of Romania and is currently residing near Bucharest, Romania. Becheru, and others, both known and unknown to the Grand Jury, would use POS memory scraping malware on victim servers located in the United States and elsewhere to illegally obtain credit card information. Becheru would then use online carding forums to sell the illegally obtained credit card information.

10. Becheru illegally obtained and sold credit card information for millions of credit cards. At one point, Becheru was in the possession of information for over 240,000 credit cards belonging to victims located in the Northern District of Texas and elsewhere.

Count One

Conspiracy to Commit Fraud and related activity in connection with access devices
(Violation of 18 U.S.C. § 371 (18 U.S.C. § 1029(a)(3)))

11. The Grand Jury realleges and incorporates by reference the allegations contained in paragraph 1 through 10 of this indictment, as if fully set forth herein.

12. Beginning on or about March 2016, and continuing until at least May 2018, in the Northern District of Texas, and elsewhere, the defendant, **Sorin Becheru**, who will be first brought to the Northern District of Texas, did knowingly combine, conspire, confederate, and agree with other persons both known and unknown to the grand jury to commit certain offenses against the United States, to wit: Fraud and related activity in connection with access devices, in violation of Title 18, United States Code, Section 1029(a)(3).

Manner and Means of the Conspiracy

13. It was part of the conspiracy for the defendant and other persons to unlawfully enrich themselves, by fraudulently gaining access, without authorization, to protected computers around the world. The defendant and others would then exfiltrate and scrape credit card information from those protected computers and sell the information in online carding forums. Coconspirator buyers would purchase the credit card information from the defendant and fraudulently use them to purchase goods and services in the Northern District of Texas and elsewhere.

Overt Acts

14. In furtherance of the conspiracy and to effect the objects of the conspiracy, the following overt acts, among others, were committed in the Northern District of Texas

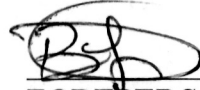
and elsewhere by the defendant and his coconspirators:

- a. On or about October 29, 2017, Becheru using the username “T0r@creep.im” messaged username “xff0dc0a” and passed the IP address and login credentials for victim server P.S. located in the United States for the purpose of scraping credit card information.
- b. Between on or about October 17, 2017, and on or about April 23, 2018, Becheru using username “buchetta@jabbb3r.de,” had conversations with “Insider@xmpp.jp” and “barcelona1986@default.rs,” about reviewing and updating the online carding forum “Vendetta.”
- c. On or about March 19, 2018, and March 29, 2018, Becheru using the username “turan1@jabbim.com” messaged a federal agent located in the Northern District of Texas, and passed the IP address and login credentials for victim server P.S. located in the United States for the purpose of scraping credit card information.
- d. On or about March 27, 2018, Becheru using the username “turan1@jabbim.com” messaged a federal agent located in the Northern District of Texas, and passed the IP address and login credentials for victim server L.P. located in the United Arab Emirates for the purpose of scraping credit card information.
- e. On or about April 19, 2018, Becheru accessed <https://card-ok.com/go.php> to check the usability of 14 different credit card numbers.

- f. Starting on or about April 19, 2018, Becheru using the username “buchetta@jabbb3r.de” messaged “iamadvanced@jabber.ru” and discussed the use of a POS memory scraping malware on victim servers.
- g. On or about April 30, 2018, Becheru accessed known online carding forums “Vendetta” and “Tony Montana,” for the purpose of selling credit card information.
- h. In or around January 2018, Becheru sold a credit card number ending in 1988, that was fraudulently used by a Buyer to pay an AT&T Bill totaling \$1,149.00 in the Northern District of Texas and elsewhere.
- i. In or around March 2018, Becheru sold a credit card number ending in 3103, that was fraudulently used by a Buyer to pay for expenses at Advanced Auto, The Corner Store, and Popeye’s, totaling \$239.64 in the Northern District of Texas and elsewhere.
- j. In or around May 2018, Becheru sold a credit card number ending in 5952, that was fraudulently used by a Buyer to pay an AT&T Bill totaling \$574.56 in the Northern District of Texas and elsewhere.
- k. On or about May 24, 2018, Becheru possessed and sold at least 240,000 credit card numbers belonging to victims in the Northern District of Texas and elsewhere. Buyers of the credit card numbers used those credit cards to purchase goods and services in the Northern District of Texas and elsewhere.

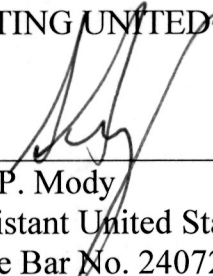
In violation of 18 U.S.C. § 371 (18 U.S.C. § 1029(a)(3)).

A TRUE BILL



FOREPERSON

PRERAK SHAH
ACTING UNITED STATES ATTORNEY



Sid P. Mody
Assistant United States Attorney
State Bar No. 24072791
1100 Commerce Street, Third Floor
Dallas, Texas 75242-1699
Facsimile: 214-659-8600
Email: siddharth.mody@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

THE UNITED STATES OF AMERICA

v.

SORIN BECHERU
a.k.a. t0r.creep.im
a.k.a. turan1@jabbim.com
a.k.a. buchetta@jabb3r.de

INDICTMENT

18 U.S.C. § 371 (18 U.S.C. § 1029(a)(3))

Conspiracy to Commit Fraud and related activity in connection with access devices

1 Count


A true bill rendered

DALLAS


FOREPERSON

Filed in open court this 2 day of March, 2021.

Warrant to be Issued


UNITED STATES MAGISTRATE JUDGE
No Criminal Matter Pending