

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

SEALED

UNITED STATES OF AMERICA

v.

CASE NO. **8:19 cr 155 T 02 JSS**

DARIY PANKOV
a/k/a "dpxaker"

18 U.S.C. § 371
18 U.S.C. § 1029(a)(2)
18 U.S.C. § 1029(a)(3)
18 U.S.C. § 1030(a)(6)

INDICTMENT

The Grand Jury charges:

COUNT ONE
(Conspiracy—18 U.S.C. § 371)

A. Introduction

At all times material to this Indictment:

1. The defendant, DARIY PANKOV, who resided in Russia, developed a malicious software program named "NLBrute." NLBrute was capable of compromising protected computers by decrypting computer passwords. PANKOV marketed and sold NLBrute and also sold thousands of login credentials for compromised computers that he had obtained through his use of NLBrute.

2. A "brute force attack" was a trial and error method used to decrypt encrypted data through exhaustive effort rather than an intellectual

2019 APR 11 PM 5:02
FILED

SEALED

strategy. Brute-forcing tools are malicious software programs, or “malware,” designed to crack computer login credentials, such as passwords.

3. The “Marketplace” was an e-commerce storefront that facilitated the unauthorized sale of computer login credentials, such as passwords, of compromised computers. The Marketplace existed primarily as a place for individuals to buy and sell access to compromised computers, which were used to facilitate a wide range of illegal activity, including tax fraud, ransomware attacks, and romance scams.

4. “Bitcoin” was digital currency generated and controlled through computer software operating on decentralized peer-to-peer networks. Because Bitcoin was transferred peer-to-peer, users could avoid traditional, regulated financial institutions, which collected information about their customers and maintained anti-money-laundering and bank-secrecy procedures.

5. “WebMoney” was an online payment settlement system. WebMoney could be used for peer-to-peer payments in several different currencies—including the U.S. Dollar (“WMZ”), Russian Ruble (“WMR”), and Bitcoin (“WMX”)—which facilitated the exchange of currencies from a single platform.

B. The Conspiracy

6. Beginning on an unknown date, but from as early as in or around June 2016, and continuing through the date of this Indictment, in the Middle District of Florida and elsewhere, the defendant,

DARIY PANKOV,
a/k/a “dpxaker,”

did knowingly and willfully combine, conspire, confederate, and agree with others known and unknown to the grand jury to commit the following offenses against the United States:

- a. fraud and related activity in connection with access devices, in violation of 18 U.S.C. § 1029(a)(2) and (a)(3); and
- b. fraud and related activity in connection with computers, in violation of 18 U.S.C. § 1030(a)(6).

C. Manner and Means

7. The manner and means by which PANKOV and others sought to accomplish the conspiracy included, among other things, the following:

- a. It was a part of the conspiracy that PANKOV would and did develop a brute-forcing malware program named NLBrute in order to compromise and obtain the login credentials of computers all over the world.

b. It was further a part of the conspiracy that PANKOV would and did advertise and offer NLBrute for sale on an online forum dedicated to computer hacking.

c. It was further a part of the conspiracy that PANKOV would and did allow conspirators to sell NLBrute on his behalf.

d. It was further a part of the conspiracy that PANKOV and his conspirators would and did require purchasers of NLBrute to use Bitcoin and WebMoney in order to conceal the identities of the conspirators.

e. It was further a part of the conspiracy that PANKOV and his conspirators would and did use NLBrute to compromise and obtain the login credentials of computers all over the world.

f. It was further a part of the conspiracy that PANKOV created an account on the Marketplace for the purpose of selling login credentials of compromised computers.

g. It was further a part of the conspiracy that PANKOV would and did list the login credentials of compromised computers for sale on the Marketplace, ultimately listing the login credentials of more than 35,000 compromised computers.

h. It was further a part of the conspiracy that PANKOV would and did obtain proceeds of this fraudulent scheme for his own personal enrichment, withdrawing \$358,437 in illicit proceeds from the Marketplace from on or about August 14, 2016 until January 15, 2019.

D. Overt Acts

8. In furtherance of the conspiracy and to effect its objects, PANKOV or his conspirators committed the following overt acts, among others, in the Middle District of Florida and elsewhere:

a. On or about June 20, 2016, PANKOV advertised the capabilities and specifications of NLBrute on an online forum dedicated to computer hacking, and he offered the malware for sale on that forum for \$250 in WMX (Bitcoin) or WMZ (U.S. Dollars).

b. On or about August 1, 2016, PANKOV sold NLBrute to a conspirator for \$250 in WMZ (Bitcoin).

c. On or about August 14, 2016, PANKOV created a username on the Marketplace for the purpose of selling access to compromised computers.

d. On or about August 14, 2016, PANKOV told a conspirator that he had access to the login credentials of approximately 3,000 compromised computers, including computers located in the United States,

France, United Kingdom, Italy, and Australia, and that he could obtain more by employing a brute-force method.

e. On or about November 4, 2016, PANKOV described himself as the “author” of NLBrute on an online forum dedicated to computer hacking, and he identified a conspirator (“Conspirator #1”) who had permission to sell the malware.

f. On or about January 2, 2018, PANKOV listed the credentials, including a password, of a law firm in the Middle District of Florida (“Firm A”) for sale on the Marketplace for \$50.

g. On or about January 3, 2018, an undercover law-enforcement officer purchased the credentials of Firm A from the Marketplace.

h. On or about March 14, 2018, an undercover law-enforcement officer purchased NLBrute from Conspirator #1 for \$250 in Bitcoin.

i. On or about June 10, 2018, PANKOV listed the credentials, including a password, of a law firm in the Middle District of Florida (“Firm B”) for sale on the Marketplace for \$19.25.

j. On or about June 15, 2018, an undercover law-enforcement officer purchased the credentials of Firm B from the Marketplace.

All in violation of 18 U.S.C. § 371.

COUNT TWO
(Trafficking in Unauthorized Access Devices—18 U.S.C. § 1029(a)(2))

1. The grand jury realleges and incorporates by reference Paragraphs 1 through 8 of Count One of this Indictment as if fully set forth herein.

2. From on or about January 1, 2017, through on or about December 31, 2017, in the Middle District of Florida and elsewhere, the defendant,

DARIY PANKOV,
a/k/a “dpxaker,”

knowingly and with the intent to defraud, trafficked in unauthorized access devices, that is, passwords of compromised computers, and by such conduct obtained a thing of value totaling \$1,000 or more, and such trafficking affected interstate and foreign commerce.

In violation of 18 U.S.C. § 1029(a)(2) and (c)(1)(A)(i).

COUNT THREE
(Trafficking in Unauthorized Access Devices—18 U.S.C. § 1029(a)(2))

1. The grand jury realleges and incorporates by reference Paragraphs 1 through 8 of Count One of this Indictment as if fully set forth herein.

2. From on or about January 1, 2018, through on or about

December 31, 2018, in the Middle District of Florida and elsewhere, the defendant,

DARIY PANKOV,
a/k/a “dpxaker,”

knowingly and with the intent to defraud, trafficked in unauthorized access devices, that is, passwords of compromised computers, and by such conduct obtained a thing of value totaling \$1,000 or more, and such trafficking affected interstate and foreign commerce.

In violation of 18 U.S.C. § 1029(a)(2) and (c)(1)(A)(i).

COUNT FOUR
(Possession of 15 or More Unauthorized Access Devices—18 U.S.C. § 1029(a)(3))

1. The grand jury realleges and incorporates by reference Paragraphs 1 through 8 of Count One of this Indictment as if fully set forth herein.

2. On or about August 15, 2016, in the Middle District of Florida and elsewhere, the defendant,

DARIY PANKOV,
a/k/a “dpxaker,”

knowingly and with the intent to defraud, possessed 15 or more unauthorized access devices, that is, passwords of compromised computers, and such possession affected interstate and foreign commerce.

In violation of 18 U.S.C. § 1029(a)(3) and (c)(1)(a)(i).

COUNT FIVE
(Possession of 15 or More Unauthorized Access Devices—18 U.S.C. § 1029(a)(3))

1. The grand jury realleges and incorporates by reference Paragraphs 1 through 8 of Count One of this Indictment as if fully set forth herein.

2. On or about October 26, 2018, in the Middle District of Florida and elsewhere, the defendant,

DARIY PANKOV,
a/k/a “dpxaker,”

knowingly and with the intent to defraud, possessed 15 or more unauthorized access devices, that is, passwords of compromised computers, and such possession affected interstate and foreign commerce.

In violation of 18 U.S.C. § 1029(a)(3) and (c)(1)(a)(i).

COUNT SIX
(Trafficking in Computer Passwords—18 U.S.C. § 1030(a)(6))

1. The grand jury realleges and incorporates by reference Paragraphs 1 through 8 of Count One of this Indictment as if fully set forth herein.

2. On or about the January 2, 2018, in the Middle District of Florida and elsewhere, the defendant,

DARIY PANKOV,
a/k/a “dpxaker,”

knowingly and with the intent to defraud trafficked in a password and similar information through which a computer may be accessed without authorization, and such trafficking affected interstate and foreign commerce.

In violation of 18 U.S.C. § 1030(a)(6)(A) and (c)(2)(A).

COUNT SEVEN
(Trafficking in Computer Passwords—18 U.S.C. § 1030(a)(6))

1. The grand jury realleges and incorporates by reference Paragraphs 1 through 8 of Count One of this Indictment as if fully set forth herein.

2. On or about the June 10, 2018, in the Middle District of Florida and elsewhere, the defendant,

DARIY PANKOV,
a/k/a “dpxaker,”

knowingly and with the intent to defraud trafficked in a password and similar information through which a computer may be accessed without authorization, and such trafficking affected interstate and foreign commerce.

In violation of 18 U.S.C. § 1030(a)(6)(A) and (c)(2)(A).

FORFEITURE

1. The allegations contained in Counts One through Seven of this Indictment are incorporated by reference as if fully set forth herein for the purpose of alleging forfeitures pursuant to 18 U.S.C. §§ 982(a)(2)(B), 1029(c)(1)(C), and 1030(i).

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 defendant,

DARIY PANKOV,
a/k/a “dpxaker,”

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 defendant,

DARIY PANKOV,
a/k/a “dpxaker,”

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. The property to be forfeited includes, but is not limited to, an order of forfeiture in the amount of \$358,437, the amount of proceeds the defendant obtained from the offenses.

5. If any of the property described above, 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,

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).

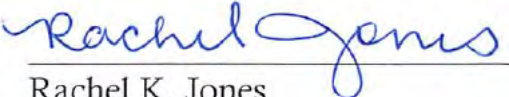
A TRUE BILL,

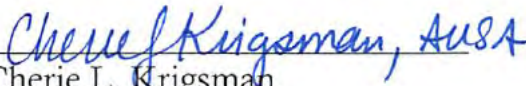


Foreperson

MARIA CHAPA LOPEZ
United States Attorney

By: 
Carlton C. Gammons
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

No.

UNITED STATES DISTRICT COURT
Middle District of Florida
Tampa Division

THE UNITED STATES OF AMERICA


vs.

DARIY PANKOV,
a/k/a "dpxaker"

INDICTMENT

Violations: 18 U.S.C. § 371
18 U.S.C. § 1029(a)(2)
18 U.S.C. § 1029(a)(3)
18 U.S.C. § 1030(a)(6)

A true bill,


Foreperson

Filed in open court this 11th day

of April 2019.


Clerk

Bail \$ _____
