

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NORTH CAROLINA
SOUTHERN DIVISION

NO. 7:22-CR-87-1M-RN

UNITED STATES OF AMERICA)
)
 v.)
)
 VYACHESLAV IGORAVICH ANDREEV)
 a/k/a "Vyacheslav Igoravich Penchukov,")
 "Tank," "Father," "TopBro," and "Zevs")
)

INDICTMENT

The Grand Jury charges:

General Allegations

At all times relevant to the indictment:

1. The defendant, VYACHESLAV IGORAVICH ANDREEV, a/k/a "Vyacheslav Igoravich Penchukov," "Tank," "Father," "TopBro," and "Zevs," was an individual residing overseas, including in Ukraine.
2. The defendant used the online nicknames "Tank," "Father," "TopBro," and "Zevs."
3. "Jabber" was a method of sending and receiving a communication over the internet.
4. "IcedID" (also known as "Bokbot") was a form of malicious software that collected and transmitted personal information from the users of infected computers, including information necessary to enter users' bank accounts. IcedID also provided

access to infected computers for other forms of malicious software, including ransomware.

5. “Ransomware” was a form of malware that encrypted a computer or computer system so that files were not accessible until a ransom was paid for a decryption key.

6. A “botnet” was a network of computers infected with malware that allowed a third party to control the entire computer network without the knowledge or consent of the computer owners. Each of the infected computers was referred to as a “bot.”

7. An “IcedID panel” was an internet-accessible database for searching IcedID victim information.

8. Victim No. 1 and Victim No. 2 were entities with offices in the Eastern District of North Carolina.

COUNT ONE

9. Paragraphs 1 through 8 are re-alleged and incorporated herein as though fully set forth in this count.

Object of the Conspiracy

10. From an unknown date, but beginning no later than in or about November 2018 and continuing through in or about April 2022, in the Eastern District of North Carolina and elsewhere, the defendant, VYACHESLAV IGORAVICH ANDREEV, a/k/a “Vyacheslav Igoravich Penchukov,” “Tank,” “Father,” “TopBro,” “Zevs,” did knowingly conspire, combine, confederate, and agree, with other

individuals, both known and unknown to the Grand Jury, to commit offenses against the United States, that is:

- a. To knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, and attempt to do so, thus having caused, and would, if completed, have caused, damage affecting 10 or more protected computers during a one year period, all in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (b), (c)(4)(A)(i)(VI), and (c)(4)(B); and
- b. To intentionally access a computer without authorization, and thereby obtain information from a protected computer, and attempt to do so, for purposes of commercial advantage and private financial gain, all in violation of Title 18, United States Code, Sections 1030(a)(2), (b), and (c)(2)(B)(i).

Manner and Means

11. Members of the conspiracy used the following manner and means, among others, to accomplish the objects of the conspiracy through the development, administration, and use of IcedID:

- a. Distributed spam emails containing malicious attachments that, when clicked, provided access to a victim computer.
- b. Identified when victims attempted to communicate with websites of interest, such as websites for major financial institutions, and

redirected the victims to websites controlled by members of the conspiracy that appeared to be the legitimate websites.

- c. Used the redirected websites to fraudulently obtain personal information from the users of infected computers, such as information necessary to enter users' bank accounts.
- d. Transmitted and stored personal information from the users of infected computers to one of a number of panels controlled by the conspirators.
- e. Used the personal information to obtain access to financial and other victim accounts and transfer money to accounts controlled by the conspirators.
- f. Used access to victim computers to download other forms of malicious software, including ransomware, onto those victim computers.

Overt Acts

12. In furtherance of the conspiracy and to effect the objects thereof, a member of the conspiracy committed at least one the following overt acts in the Eastern District of North Carolina and elsewhere:

- a. On or about November 28, 2018, a member of the conspiracy registered the username "TopBro" on an IcedID panel.
- b. On or about August 10, 2020, a member of the conspiracy caused IcedID malware to be transmitted to an email account belonging

to Victim No. 1, which was received in Wilmington, North Carolina.

- c. From an unknown date, but no later than in or about November 2018 until in or about February 2021, a member of the conspiracy managed a botnet that consisted of victim computers infected by IcedID.
- d. On or about February 25, 2021, a member of the conspiracy caused IcedID malware to be transmitted to an email account belonging to Victim No. 2, which was received in Cary, North Carolina.
- e. From an unknown date, but no later than in or about November 2018 until in or about November 2021, a member of the conspiracy used IcedID panel information to steal money from victim accounts at two financial services firms.

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

COUNT TWO

13. Paragraphs 1 through 8 are re-alleged and incorporated herein as though fully set forth in this count.

14. From an unknown date, but beginning no later than in or about November 2018 and continuing through in or about April 2022, in the Eastern District of North Carolina and elsewhere, the defendant, VYACHESLAV IGORAVICH ANDREEV, a/k/a “Vyacheslav Igoravich Penchukov,” “Tank,” “Father,”

“TopBro,” “Zevs,” did knowingly and willfully combine, conspire, confederate, and agree with one or more persons, known and unknown to the Grand Jury, to commit an offense against the United States, that is: to knowingly devise and intend to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing the same, to transmit or cause to be transmitted by means of wire communications in interstate and foreign commerce certain writings, signs, signals, pictures, and sounds, in violation of Title 18, United States Code, Section 1343.

Purpose of the Conspiracy

15. The primary purpose of the conspiracy and the scheme and artifice was to obtain money and property from victims by using IcedID to gain access to victim bank accounts and transfer their money to accounts controlled by the conspirators. It was also the purpose of the conspiracy for the conspirators to financially benefit from providing access to victim computers to other forms of malware, including ransomware, to allow that malware to defraud the victims.

Manner and Means

16. Paragraph 11 is re-alleged and incorporated herein as though fully set forth in this count.

17. It was a further part of the conspiracy and scheme and artifice that the conspirators communicated with each other by and through wire communications in interstate and foreign commerce, including through Jabber.

18. It was a further part of the conspiracy and scheme and artifice that on or about November 28, 2018, a member of the conspiracy registered the username "TopBro" on an IcedID panel.

19. It was a further part of the conspiracy and scheme and artifice that on or about August 10, 2020, a member of the conspiracy caused IcedID malware to be transmitted to an email account belonging to Victim No. 1, which was received in Wilmington, North Carolina.

20. It was a further part of the conspiracy and scheme and artifice that on or about February 25, 2021, a member of the conspiracy caused IcedID malware to be transmitted to an email account belonging to Victim No. 2, which was received in Cary, North Carolina.

21. It was a further part of the conspiracy and scheme and artifice that from an unknown date, but no later than in or about November 2018 until in or about February 2021, a member of the conspiracy managed a botnet for IcedID.

22. It was a further part of the conspiracy and scheme and artifice that from an unknown date, but no later than in or about November 2018 until in or about November 2021, a member of the conspiracy used IcedID panel information to communicate with computers at two financial services firms in order to steal money from victim accounts.

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

FORFEITURE

Notice is hereby given that all right, title and interest in the property described herein is subject to forfeiture.

Upon conviction of any offense charged herein constituting “specified unlawful activity” (as defined in 18 U.S.C. §§ 1956(c)(7) and 1961(1)), or a conspiracy to commit such offense, the defendant shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C), as made applicable by 28 U.S.C. § 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the said offense.

Upon conviction of any violation of, or conspiracy to violate, Section 1030 of Title 18 of the United States Code, the defendant shall forfeit to the United States, pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i)(1)(B), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of the said offense, or, pursuant to 18 U.S.C. § 1030(i)(1)(A), any personal property that was used or intended to be used to commit or to facilitate the commission of the said offense.

If any of the above-described forfeitable property, as a result of any act or omission of a defendant: cannot be located upon the exercise of due diligence; has been transferred or 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; it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p),

to seek forfeiture of any other property of said defendant up to the value of the forfeitable property described above.

A TRUE BILL

FOR PERSON


REDACTED VERSION

Pursuant to the E-Government Act and the federal rules, the unredacted version of this document has been filed under seal.

DATE

7-21-2022

MICHAEL F. EASLEY, JR.
United States Attorney


BY: BRADFORD M. DEVOE
Assistant United States Attorney

RYAN K.J. DICKEY
Senior Counsel
Criminal Division, Computer Crime and Intellectual Property Section