

SEALED

ORIGINAL

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

FILED-USDC-NDTX-DA
'24 SEP 24 PM3:53
LMB

UNITED STATES OF AMERICA

v.

IANIS ALEKSANDROVICH
ANTROPENKO

3 - 24 CR - 402 - L
NO. 3:24-CR-
FILED UNDER SEAL

INDICTMENT

The Grand Jury Charges:

At times material to this Indictment:

Introduction

1. The defendant **Ianis Aleksandrovich Antropenko** is a citizen of Russia who has resided in the United States from at least 2019 to the present.
2. Victim Company 1 (“VC1”) is a data analysis company located in the Dallas Division of the Northern District of Texas.
3. Adult Victim 1 (“AV1”) is the President and Chief Executive Officer of VC1 residing in the Dallas Division of the Northern District of Texas.
4. Ransomware is a type of malware that allows a perpetrator to encrypt some or all of the data stored on a victim computer and transmit some or all of the victim’s data to another computer under the perpetrator’s control. After a ransomware attack, a perpetrator typically demands a ransom payment from the victim in exchange for

decrypting the victim's data, refraining from publishing the data, deleting the perpetrator's copy of the victim's stolen data, or any combination thereof.

5. From at least 2019 through at least 2022, perpetrators have used the Zeppelin ransomware to target a wide range of businesses and critical infrastructure organizations, including defense contractors, educational institutions, manufacturers, technology companies, and healthcare and medical industry organizations. Perpetrators using Zeppelin ransomware have been known to request ransom payments in Bitcoin, with amounts ranging from several thousand dollars to over a million dollars.

6. Perpetrators using Zeppelin ransomware gain access to victim networks through various methods such as Remote Desktop Protocol ("RDP") exploitation, firewall vulnerabilities exploitation, and phishing campaigns. Once the perpetrators gain access to the network, deploy, and execute the Zeppelin ransomware, a ransom note is left on the compromised system, frequently on the desktop. This ransom note contains instructions on how to make contact with the perpetrators in order to decrypt the stolen data.

Count One

Conspiracy to Commit Computer Fraud and Abuse
(Violation of 18 U.S.C. § 371)

7. The Grand Jury realleges and incorporates by reference the allegations contained in Paragraphs 1 through 6 of this Indictment as if fully set forth herein.

8. From at least on or about May 6, 2018, to at least on or about August 19, 2022, in the Dallas Division of the Northern District of Texas and elsewhere, the defendant, **Ianis Aleksandrovich Antropenko**, did conspire and agree with other persons known and unknown to the Grand Jury to knowingly cause the transmission of a program, information, code, and command, and as a result, intentionally cause damage, without authorization, to a protected computer, and (i) cause loss to 1 or more persons during a one-year period from the defendant's course of conduct affecting 1 or more other protected computers aggregating at least \$5,000 in value, and (ii) cause damage affecting 10 or more protected computers during a one-year period, in violation of 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(A)(i)(I), 1030(c)(4)(A)(i)(VI), and 1030(c)(4)(B)(i).

Object of the Conspiracy

9. The object of the conspiracy was for **Antropenko** and others to unlawfully enrich themselves by receiving financial compensation for perpetrating and aiding and abetting ransomware attacks on computers located throughout the United States and elsewhere, including the Dallas Division of the Northern District of Texas.

Overt Acts

10. In furtherance of the conspiracy and to accomplish its objects, **Antropenko**, together with others, did commit and cause the commission of the following overt acts, among others, in the Northern District of Texas and elsewhere:

- a. On or about May 6, 2018, **Antropenko** registered the china.helper@aol.com email address.
- b. On or about January 4, 2021, **Antropenko** and his co-conspirators used the Zeppelin ransomware to encrypt, without authorization, files on computers belonging to VC1 and AV1, which were located in the Dallas Division of the Northern District of Texas.
- c. On or about January 6, 2021, **Antropenko** and his co-conspirators emailed representatives of VC1 demanding payment in Bitcoin in order to decrypt the encrypted files.

All in violation of 18 U.S.C. § 371.

Count Two

Computer Fraud and Abuse

(Violation of 18 U.S.C. §§ 2, 1030(a)(5)(A), 1030(c)(4)(A)(i)(I), 1030(c)(4)(B)(i))

11. The Grand Jury realleges and incorporates by reference the allegations contained in Paragraphs 1 through 6 and 9 through 10 of this Indictment as if fully set forth herein.

12. From on or about December 22, 2020, to on or about January 21, 2021, in the Dallas Division of the Northern District of Texas and elsewhere, the defendant, **Ianis Aleksandrovich Antropenko**, knowingly caused the transmission of a program, information, code, and command, and as a result, intentionally caused damage, without authorization, to a protected computer, and caused loss to 1 or more persons during a one-year period from the defendant's course of conduct affecting 1 or more other protected computers aggregating at least \$5,000 in value, to wit: Antropenko caused and aided and abetted the encryption of files on the computers of VC1 and AV1 using the Zeppelin ransomware, which then cost the company over \$5,000 to decrypt the files.

In violation of 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(A)(i)(I), 1030(c)(4)(B)(i), and 2.

Count Three
Conspiracy to Commit Money Laundering
(Violation of 18 U.S.C. §§ 1956(h) & 1956(a)(1)(B)(i) and (ii))

13. The Grand Jury realleges and incorporates by reference the allegations contained in Paragraphs 1 through 6 and 9 through 10 of this Indictment as if fully set forth herein.

14. From on or about May 6, 2018, to at least on or about August 19, 2022, in the Dallas Division of the Northern District of Texas and elsewhere, the defendant, **Ianis Aleksandrovich Antropenko**, did knowingly combine, conspire, and agree with other persons known and unknown to the Grand Jury to commit offenses against the United States in violation of Title 18, United States Code, Section 1956, to wit: to knowingly conduct and attempt to conduct financial transactions affecting interstate commerce and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, computer fraud and abuse as prohibited by 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B)(i), 1030(c)(4)(A)(i)(I) and 1030(c)(4)(A)(i)(VI), knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, and knowing that the transactions were designed in whole or in part:

- to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, in violation of 18 U.S.C. § 1956(a)(1)(B)(i); and
- to avoid a transaction reporting requirement under State or Federal law, in violation of 18 U.S.C. § 1956(a)(1)(B)(ii).

Manner and Means of the Conspiracy

15. The manner and means used to accomplish the objectives of the conspiracy included, among others, the following:

- a. ANTROPENKO participated in the conspiracy described in Count One and committed the crime described in Count Two, including aiding and abetting the attack against VC1 and AV1 in the Northern District of Texas and other substantive offenses of computer fraud and abuse, in order to generate funds that could be laundered;
- b. ANTROPENKO and Co-Conspirator 1 sent payments received from victims of computer fraud and abuse, including funds transmitted by VC1 and AV1, to an illicit cryptocurrency mixing service in order to obfuscate their nature, location, source, ownership, and control, and then to cryptocurrency exchange accounts held by ANTROPENKO and Co-Conspirator 1;
- c. ANTROPENKO would arrange physical exchanges of cryptocurrency for cash with persons in the United States using encrypted messaging applications;
- d. ANTROPENKO would deposit the cash in a bank account he controlled using structured deposits;
- e. ANTROPENKO and Co-Conspirator 1 agreed that Co-Conspirator 1 would store a disguised copy of a seed phrase in an account belonging to Co-

Conspirator 1. This seed phrase was for a cryptocurrency wallet used to launder funds for the conspiracy and would allow Co-Conspirator 1 to continue having access to the funds should anything happen to ANTROPENKO;

In violation of 18 U.S.C. §§ 1956(h) and 1956(a)(1)(B)(i) and (ii).

Forfeiture Notice

(18 U.S.C. § 982(a)(2)(B); 18 U.S.C. § 1030(i)(1); 18 U.S.C. § 982(a)(1))

16. Upon conviction on Counts One and Two of this Indictment, the defendant, **Ianis Aleksandrovich Antropenko**, shall forfeit to the United States (i) pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i)(1), any property constituting, or derived from, proceeds obtained directly or indirectly, as the result of the violation; and (ii) pursuant to 18 U.S.C. § 1030(i)(1), any personal property that was used or intended to be used to commit or to facilitate the commission of the violation.

17. Upon conviction on Count Three of this Indictment, the defendant, **Ianis Aleksandrovich Antropenko**, shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(1), any property, real or personal, involved in the offense, and any property traceable to such property.

18. The property subject to forfeiture includes, but is not limited to, the following:

- a. \$70,900 in United States Currency seized pursuant to a warrant executed at 7725 Gateway, Apt. 4552, Irvine, CA 92618 on February 13, 2024.
- b. A Lexus RX350 with VIN JT[...]94 seized pursuant to a warrant executed at 7725 Gateway, Apt. 4552, Irvine, CA 92618 on February 13, 2024.
- c. Various cryptocurrency (approximately 0.39 ETH, 1,447,841.26 USDT, and 677,173.7 USDC) seized from the cryptocurrency wallet 0x[...]98 pursuant to a warrant executed in the Northern District of Texas on February 13, 2024.

19. If any of the property described above, as a result of any act or omission of

Indictment—Page 9

the 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 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. §§ 982(b)(1) and 1030(i)(2), to seek forfeiture of any other property of the defendant, up to the value of the property described above.


A TRUE BILL.


FOREPERSON

LEIGHA SIMONTON
United States Attorney
Northern District of Texas


JONGWOO CHUNG
Assistant United States Attorney
NC Bar No. 52070
1100 Commerce Street, Third Floor
Dallas, Texas 75242-1699
Telephone: 214-659-8600
Facsimile: 214-659-8806
Email: jongwoo.chung@usdoj.gov

NICOLE ARGENTIERI
Principal Deputy Assistant Attorney General
Criminal Division


BENJAMIN A. BLEIBERG
Trial Attorney
DC Bar No. 90006584
1301 New York Avenue NW
Washington, D.C. 20530
Telephone: 202-514-1026
Facsimile: 202-514-6113
Email: benjamin.bleiberg@usdoj.gov

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

THE UNITED STATES OF AMERICA

v.

IANIS ALEKSANDROVICH ANTROPENKO

SEALED INDICTMENT

18 U.S.C. § 371
Conspiracy to Commit Computer Fraud and Abuse
(Count 1)

18 U.S.C. §§ 2, 1030(a)(5)(A), 1030(c)(4)(A)(i)(I), 1030(c)(4)(B)(i)
Computer Fraud and Abuse
(Count 2)

18 U.S.C. §§ 1956(h) & 1956(a)(1)(B)(i) and (ii)
Conspiracy to Commit Money Laundering
(Count 3)

18 U.S.C. § 982(a)(2)(B); 18 U.S.C. § 1030(i)(1); 18 U.S.C. § 982(a)(1)
Forfeiture Notice

3 Counts

A true bill rendered

DALLAS



FOREPERSON

Filed in open court this 24th day of September, 2024.

Warrant to be Issued



UNITED STATES MAGISTRATE JUDGE
No Criminal Matter Pending