

ORIGINAL

SEALED

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

CLERK US DISTRICT COURT
NORTHERN DIST. OF TX
FILED

2021 AUG 11 PM 2:41

UNITED STATES OF AMERICA

CRIMINAL NO. DEPUTY CLERK ✓

V.

3-21CR0366-S

Yaroslav Vasinskyi (01)
a/k/a Profcomserv
a/k/a Rabotnik
a/k/a Rabotnik_New
a/k/a Yarik45
a/k/a Yaroslav2468
a/k/a Affiliate 22

FILED UNDER SEAL

INDICTMENT

The Grand Jury charges:

At all times material to this indictment:

General Allegations

1. "Malware" was a malicious software program designed to disrupt computer operations, gather sensitive information, gain access to private computer systems, and perform other unauthorized actions on computer systems. Common examples of malware included viruses, ransomware, worms, keyloggers, and spyware.

2. "Ransomware" was a type of malware that infected a computer and encrypted some or all of the data on the computer. Distributors of ransomware typically extorted the user of the encrypted computer by demanding that the user pay a ransom in order to decrypt and recover the data on the computer.

3. “Sodinokibi” was a form of ransomware that encrypted victim computers. Sodinokibi was given other names, such as REvil. Distributors of Sodinokibi ransomware were also known as “affiliates.”

4. “Bitcoin” was a type of virtual currency, circulated over the Internet as a form of value. Bitcoin were not issued by any government, bank, or company, but were generated and controlled through computer software operating via a decentralized, peer-to-peer network. To acquire Bitcoin, a user typically purchased Bitcoin from a Bitcoin seller or “exchanger.”

5. “Bitcoin addresses” were particular locations to which Bitcoin were sent and received. A Bitcoin address was analogous to a bank account number and was represented as a 26-to-35 character-long case-sensitive string of letters and numbers. Each Bitcoin address was controlled through the use of a unique corresponding private key which was a cryptographic equivalent of a password and was needed to access the Bitcoin address. Only the holder of a Bitcoin address’s private key could authorize a transfer of Bitcoin from that address to another Bitcoin address. Little to no personally identifiable information about a Bitcoin account holder was transmitted during a Bitcoin transaction.

6. A “command and control server” was a centralized computer that issued commands to remotely connected computers. “Command and Control” (“C2”) infrastructure consisted of servers and other technical infrastructure that issued commands to control malware.

7. Computer programs, including malware, were written in computer programming languages which included “Ruby,” “C,” and “C++.”

8. “Encryption” was the translation of data into a secret code. In order to access encrypted data, a user must have accessed a password, commonly referred to as a “decryption key” or “decryptor” that enabled the user to decrypt the data.

9. A “Gitlab server” was a server that can be used to create and manage software and coding projects.

10. “Monero” was a type of virtual currency, circulated over the Internet as a form of value. Monero was not issued by any government, bank, or company. To acquire Monero, a user typically purchased Monero from a virtual currency “exchanger.” Monero transaction details were anonymous. Therefore, the final destination address could not be traced and the receiving participant could not be identified from the Monero transaction details alone.

11. “Phishing” was a process where specially-crafted emails were distributed to recipients with a purpose of collecting the recipients’ credentials and delivering malware.

12. Remote desktop tools were computer programs that provided a user with a graphical user interface to connect to another computer over a network connection.

13. “Security vulnerabilities” were unintended flaws in software code or an operating system that left a computer open to exploitation in the form of unauthorized access and malicious behavior (e.g., the deployment of malware).

14. Tor was a computer network designed to facilitate anonymous communication over the Internet. The Tor network did this by routing a user’s

communications through a globally-distributed network of relay computers in a manner that rendered ineffective any conventional Internet Protocol (“IP”) based methods of identifying users. The Tor network also enabled users to operate hidden sites that operated similarly to conventional websites.

15. A virtual private server (“VPS”) was a virtual machine sold as a server by an internet hosting service that allows individuals to lease space on a server as their own.

16. Entity A was an entity located in Braintree, Massachusetts.

17. Company B was a business located in Miami, Florida.

18. Company C was a business located in Yonkers, New York.

19. Company D was a financial institution located in Dallas, Texas which was located in the Northern District of Texas.

20. Company E was a business located in located in Addison, Texas which was located in the Northern District of Texas.

21. Company F was a business located in Dallas, Texas which was located in the Eastern District of Texas.

22. Company G was a business located in Stamford, Connecticut.

23. Company H was a business located in La Plata, Maryland.

24. Company I was a business located in Fairfield, New Jersey.

25. Company J was a business located in Tempe, Arizona.

26. Defendant **Yaroslav Vasinskyi** was a citizen of Ukraine. **Vasinskyi** used various online monikers including, Profcomserv, Rabotnik, Rabotnik_New, Yarik45, Yaroslav2468, and Affiliate 22.

Count One

Conspiracy to Commit Fraud and Related Activity in Connection with Computers
[Violation of 18 U.S.C. § 371 (18 U.S.C. §§ 1030(a)(5)(A) and 1030(a)(7)(C)]

27. Paragraphs 1 through 26 of this indictment are re-alleged and incorporated by reference as though fully set forth herein.

28. From on or about March 1, 2019, through on or about August 11, 2021, in the Northern District of Texas and elsewhere, defendant **Yaroslav Vasinskyi** did knowingly and willfully combine, conspire, confederate, and agree with others known and unknown to the Grand Jury, to commit an offense 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 cause loss to persons during a 1-year period from the defendant's course of conduct affecting protected computers aggregating at least \$5,000 in value, and cause damage affecting 10 or more protected computers during a 1-year period, in violation of 18 U.S.C.

§§ 1030(a)(5)(A) and 1030(c)(4)(B); and

b. to knowingly and with intent to extort from any person any money and other thing of value, transmit in interstate and foreign commerce any communication containing a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, in violation of 18 U.S.C. §§ 1030(a)(7)(C) and 1030(c)(3)(A).

Purpose of the Conspiracy

29. It was the purpose of the conspiracy for defendant **Yaroslav Vasinskyi** and other conspirators to unlawfully enrich himself and others by: (a) authoring Sodinokibi ransomware that would, when executed, encrypt data on victims' computers; (b) conducting reconnaissance and research in order to target potential victims; (c) accessing victims' computers without authorization through phishing, remote desktop exploitation, and security vulnerabilities; (d) installing and executing Sodinokibi ransomware on victims' computers, resulting in the encryption of data on the computers; (e) extorting victims by demanding a ransom paid in Bitcoin and Monero in exchange for decryption keys to decrypt the data; and (f) collecting ransom payments from victims who paid the ransom.

Manner and Means of the Conspiracy

30. The manner and means by which defendant **Yaroslav Vasinskyi** and other conspirators sought to accomplish the purpose of the conspiracy included, among other things:

- a. Conspirators authored Sodinokibi ransomware, which was designed to encrypt data on victims' computers. Conspirators deployed the first operational version of Sodinokibi ransomware in or about April 2019. Since then, conspirators regularly have updated Sodinokibi ransomware and refined the manner in which Sodinokibi attacks are conducted.
- b. Conspirators infected victims' computers in various ways, including by deploying phishing emails to collect the recipients' credentials and to deliver

malware, by using compromised remote desktop credentials, and by exploiting security vulnerabilities in software code and operating systems. Once conspirators accessed victims' computers, conspirators sought to obtain persistent remote access to the compromised networks.

c. Through this persistent remote access, the conspirators then used malware, including types named Cobalt Strike, Metasploit, and Mimikatz, to gain further access and control of other computers in the victims' networks in order to elevate access to administrator privileges on the victims' networks.

d. After gaining sufficient privileges and access to the computers in the victims' networks, the conspirators located backups and attempted to delete and encrypt the backups. Thereafter, the conspirators deployed Sodinokibi ransomware on the victims' networks. Beginning in or about January 2020, conspirators began exfiltrating the victims' data prior to deploying the Sodinokibi ransomware. Once exfiltrated, the conspirators posted portions of the data on a blog to (1) prove they had taken the victims' data, and (2) to threaten publication of all the victims' data if the ransom was not paid.

e. Through deployment of the Sodinokibi ransomware by the conspirators, the files on the victims' computers were encrypted. Further, through the deployment of Sodinokibi ransomware, the conspirators left an electronic note in the form of a text file on the victims' computers. The note included a Tor website address and an unencrypted website address for the victims to visit in order to have the victims' files decrypted.

f. Upon going to either the Tor website or the unencrypted website, victims were given the ransom amount demanded and provided a virtual currency address to use to pay the ransom. The websites also had a countdown timer denoting the time by which the ransom had to be paid before the ransom amount increased. The websites included a chat feature through which the victims could communicate with Sodinokibi conspirators.

g. At times, during the course of communications, the conspirators negotiated the ransom amount with the victims and the victims' representatives. Further, at times the conspirators decrypted a file to prove that the decryption key worked.

h. In the event a victim paid the ransom amount, the conspirators provided the decryption key to the victims, and the victims then were able to access their files. In the event a victim did not pay the ransom, the conspirators typically posted the victims' exfiltrated data or claimed that they sold the exfiltrated data to third parties.

Overt Acts

31. In furtherance of the conspiracy and to affect its unlawful objects, defendant **Yaroslav Vasinskyi** and other conspirators committed and caused to be committed the following overt acts in the Northern District of Texas and elsewhere:

a. On or about May 21, 2019, defendant **Yaroslav Vasinskyi** and other conspirators accessed the internal computer networks of Entity A without authorization.

- b. On or about May 21, 2019, defendant **Yaroslav Vasinskyi** and other conspirators deployed Sodinokibi ransomware on Entity A's computers thereby encrypting Entity A's computers.
- c. On or about May 21, 2019, defendant **Yaroslav Vasinskyi** and other conspirators transmitted in interstate and foreign commerce a ransom demand in relation to encrypting Entity A's computers demanding approximately \$499,800 in exchange for a decryption key to decrypt the data.
- d. On or about July 4, 2019, a conspirator using the moniker "Unknown" posted an advertisement soliciting individuals to interview to become affiliates for the distribution of Sodinokibi ransomware. In pertinent part, the Russian-language advertisement stated (translated) that it was "private ransomware written in C," and that the affiliate would initially receive 60%, and then 70% after three ransom payments.
- e. On or about December 14, 2019, defendant **Yaroslav Vasinskyi** sent a message on a criminal forum to "Unknown." **Vasinskyi** wrote in Russian (translated), "Hello, this is rabotnik. I want to return to work."
- f. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators accessed the internal computer networks of Company B without authorization and caused damage.
- g. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators accessed the internal computer networks of Company C without authorization and caused damage.

- h. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators accessed the internal computer networks of Company C's clients without authorization.
- i. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators deployed Sodinokibi ransomware on Company C's clients thereby encrypting Company C's clients' computers.
- j. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators accessed the internal computer networks of Company D without authorization and caused damage.
- k. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators deployed Sodinokibi ransomware on Company D's computers thereby encrypting Company D's computers.
- l. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators accessed the internal computer networks of Company E without authorization and caused damage.
- m. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators deployed Sodinokibi ransomware on Company E's computers thereby encrypting Company E's computers.
- n. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators accessed the internal computer networks of Company F without authorization and caused damage.

o. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators deployed Sodinokibi ransomware on Company F's computers thereby encrypting Company F's computers.

p. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators accessed the internal computer networks of Company G without authorization and caused damage.

q. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators accessed the internal computer networks of Company G's clients without authorization.

r. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators deployed Sodinokibi ransomware on Company G's clients thereby encrypting Company G's clients' computers.

s. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators accessed the internal computer networks of Company H without authorization and caused damage.

t. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators accessed the internal computer networks of Company H's clients without authorization.

u. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators deployed Sodinokibi ransomware on Company H's clients thereby encrypting Company H's clients' computers.

- v. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators accessed the internal computer networks of Company I without authorization and caused damage.
- w. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators accessed the internal computer networks of Company I's clients without authorization.
- x. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators deployed Sodinokibi ransomware on Company I's clients thereby encrypting Company I's clients' computers.
- y. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators transmitted in interstate and foreign commerce a ransom demand of approximately \$700,000 in relation to the encryption of the computers of Company I's clients using Sodinokibi ransomware.
- z. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators accessed the internal computer networks of Company J without authorization and caused damage.
- aa. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators accessed the internal computer networks of Company J's clients without authorization.

bb. On or about July 2, 2021, defendant **Yaroslav Vasinskyi** and other conspirators deployed Sodinokibi ransomware on Company J's clients thereby encrypting Company J's clients' computers.

All in violation of 18 U.S.C. § 371 (18 U.S.C. §§ 1030(a)(5)(A) and 1030(a)(7)(C)).

Counts Two through Ten

Intentional Damage to a Protected Computer

[Violation of 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B), and 2]

32. Paragraphs 1 through 26 of this indictment are re-alleged and incorporated by reference as though fully set forth herein.

33. On or about the dates set forth below, in the Northern District of Texas and elsewhere, defendant **Yaroslav Vasinskyi**, who will be first brought to the Northern District of Texas, and others known and unknown to the Grand Jury, did knowingly cause the transmission of a program, information, code, and command and, as a result of such conduct, intentionally caused damage, and attempted to cause damage, without authorization, to a protected computer, and the offense caused loss to persons during a 1-year period from the defendant's course of conduct affecting protected computers aggregating at least \$5,000 in value, and caused damage affecting 10 or more protected computers during a 1-year period, described below for each count, each transmission consisting a separate count:

Count	Date(s)	Victim
Two	May 21, 2019	Company A
Three	July 2, 2021	Company B
Four	July 2, 2021	Company C
Five	July 2, 2021	Company D
Six	July 2, 2021	Company E
Seven	July 2, 2021	Company F
Eight	July 2, 2021	Company G

Count	Date(s)	Victim
Nine	July 2, 2021	Company H
Ten	July 2, 2021	Company I

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

Count Eleven

Conspiracy to Commit Money Laundering
[Violation of 18 U.S.C. §§ 1956(h), 1956(a)(2)(B)(i), and 1957]

34. Paragraphs 1 through 26 of this indictment are re-alleged and incorporated by reference as though fully set forth herein.

35. From on or about March 1, 2019, through on or about August 11, 2021, in the Northern District of Texas and elsewhere, defendant **Yaroslav Vasinskyi** did knowingly combine, conspire, confederate, and agree with other persons known and unknown to the Grand Jury,

a. to transport, transmit, and transfer, and attempt to transport, transmit, and transfer a monetary instrument and funds from a place in the United States, to and through a place outside the United States, knowing that the monetary instrument and funds involved in the transportation, transmission, and transfer represent the proceeds of a specified unlawful activity, namely, fraud and related activity in connection with computers, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(a)(7)(C), to conceal and disguise the nature, the location, the source, the ownership, and the control of the proceeds of the specified unlawful activity, in violation of 18 U.S.C. § 1956(a)(2)(B)(i); and

b. to knowingly engage and attempt to engage in a monetary transaction affecting interstate and foreign commerce in criminal derived property of a value greater than \$10,000, such property having been derived from a specified unlawful activity, namely, fraud and related activity in connection with computers, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(a)(7)(C), in violation of 18 U.S.C. § 1957.

All in violation of 18 U.S.C. §§ 1956(h), 1956(a)(2)(B)(i), and 1957.

Forfeiture Notice

[18 U.S.C. §§ 982(a)(2)(B), 1030(i), and 982(a)(1)]

36. Paragraphs 1 through 26 of this indictment are realleged and incorporated by reference as though fully set forth herein.

37. Upon conviction for any offense alleged in Counts One through Ten of this indictment, defendant **Yaroslav Vasinskyi** shall forfeit to the United States of America the following:

- a. Pursuant to 18 U.S.C. § 982(a)(2)(B), any property constituting, or derived from, proceeds obtained directly or indirectly, as the result of the respective violation, including a forfeiture “money” judgment.
- b. 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 respective violation, and any property, real or personal, constituting or derived from, any proceeds obtained, directly or indirectly, as a result of the respective violation, including a forfeiture “money” judgment.

38. Upon conviction for the offense alleged in Count Eleven of this indictment, defendant **Yaroslav Vasinskyi** shall forfeit to the United States of America, pursuant to 18 U.S.C. § 982(a)(1), any property, real or personal, involved in the offense, and any property traceable to that property, including a forfeiture “money” judgment.

39. Further, if any of the property described above, as a result of any act or omission of 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, the United States of America shall be entitled to forfeiture of substitute property pursuant to 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



FOREPERSON

PRERAK SHAH
ACTING UNITED STATES ATTORNEY



TIFFANY H. EGGERS
Assistant United States Attorney
Florida Bar No. 0193968
1100 Commerce Street, Third Floor
Dallas, Texas 75242-1699
Telephone: 214-659-8600
Facsimile: 214-659-8805
Email: Tiffany.Eggers@usdoj.gov



BYRON JONES
Senior Counsel
Tennessee No. 010507
Computer Crime and Intellectual Property Section
U.S. Department of Justice
Washington, D.C. 20005
Telephone: 202-514-1026
Email: Byron.Jones@usdoj.gov

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

THE UNITED STATES OF AMERICA

v.

YAROSLAV VASINSKYI

SEALED INDICTMENT

18 U.S.C. §§ 371 (18 U.S.C. §§ 1030(a)(5)(A) and 1030(a)(7)(C)
Conspiracy to Commit Fraud and Related Activity in Connection with Computers
(Count 1)

18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B), and 2
Intentional Damage to a Protected Computer
(Counts 2, 3, 4, 5, 6, 7, 8, 9, and 10)

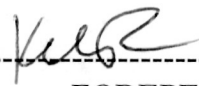
18 U.S.C. §§ 1956(h), 1956(a)(2)(B)(i), and 1957
Conspiracy to Commit Money Laundering
(Count 11)

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

11 Counts

A true bill rendered

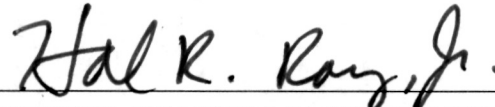
FORT WORTH



FOREPERSON

Filed in open court this 11th day of August, 2021.

Warrant to be Issued



UNITED STATES MAGISTRATE JUDGE
No Criminal Matter Pending