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

UNITED STATES OF AMERICA

v.

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

NO. 3:21-CR-366-S

FACTUAL RESUME

In support of Yaroslav Vasinskyi's plea of guilty to the offenses in Counts One through Eleven of the indictment, Vasinskyi, the defendant, Simon Kabzan and Stephen Green, the defendant's attorneys, and the United States of America (the government) stipulate and agree to the following:

ELEMENTS OF THE OFFENSE

To prove the offense alleged in **Count One** of the indictment, charging a violation of 18 U.S.C. §§ 371, 1030(a)(5)(A) and 1030(a)(7)(C), that is, Conspiracy to Commit Fraud and Related Activity in Connection with Computers, the government must prove each of the following elements beyond a reasonable doubt:[1]

> First: That the defendant and at least one other person agreed to commit the crime of Fraud and Related Activity in Connection with Computers, as charged in the indictment;

[1] Fifth Circuit Pattern Jury Instruction 2.15A (5th Cir. 2019).

> Second: That the defendant knew the unlawful purpose of the agreement and joined in it willfully, that is, with the intent to further the unlawful purpose; and
>
> Third: That at least one of the conspirators during the existence of the conspiracy knowingly committed at least one of the overt acts described in the indictment, in order to accomplish some object or purpose of the conspiracy.

Sections 1030(a)(5)(A) and (a)(7)(C) of Title 18 provide,[2]

> (a) Whoever—
>
> (5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer
>
> . . .
>
> (7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—
>
> . . .
>
> (C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;
>
> shall be punished as provided in subsection (c) of this section.

To prove the offenses alleged in **Counts Two through Ten** of the indictment, charging a violation of 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B), and 2, that is, Intentional Damage to a Protected Computer, the government must prove the following beyond a reasonable doubt:[3]

> First: The defendant knowingly caused the transmission of a program, information, code, or command; and
>
> Second: By doing so, the defendant intentionally caused damage to a

[2] There are no Fifth Circuit Pattern Jury Instructions for violations of 18 U.S.C. §§ 1030(a)(5)(A) and (a)(7)(C); therefore, the text of the statute is included here

[3] As noted above, there is no Fifth Circuit Pattern Jury Instruction for a violation of 18 U.S.C. § 1030(a)(5)(A). The statute is included above and the Seventh Circuit Pattern Instruction is included herein.

protected computer without authorization.

To prove the offense alleged in **Count Eleven** of the indictment, charging a violation of 18 U.S.C. §§ 1956(h), 1956(a)(2)(B)(i), and 1957, that is, Conspiracy to Commit Money Laundering, the government must prove the following beyond a reasonable doubt:[4]

> First: That the defendant and at least one other person made an agreement to commit the crime of laundering of monetary instruments, in violation of 18 U.S.C. § 1956(a)(2)(B)(i) and the crime of engaging in monetary transactions in property derived from specified unlawful activity, in violation of 18 U.S.C. § 1957;[5]
>
> Second: That the defendant knew the unlawful purpose of the agreement; and
>
> Third: That the defendant joined in the agreement willfully, that is, with the intent to further the unlawful purpose.

Section § 1956(a)(2)(B)(i) of Title 18 provides that:[6]

> (2) Whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States--
>
> . . .
>
> (B) knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part—
>
> (i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity;

---

[4] Fifth Circuit Pattern Jury Instruction 2.76C (5th Cir. 2019).
[5] The text of 18 U.S.C. §§ 1030(a)(5)(A) and (a)(7)(C) are included above.
[6] There are no Fifth Circuit Pattern Jury Instruction for 18 U.S.C. § 1956(a)(2)(B)(i); therefore, the text of the statute is included here.

The elements of § 1956(a)(2)(B)(i) include the following:[7]

> First: The defendant knowingly transported, transmitted, or transferred, or attempted to transport, transmit or transfer, a monetary instrument or funds; and
>
> Second: The transportation, transmittal, or transfer, or attempted transportation, transmittal, or transfer, was from a place in the United States to or through a place outside the United States;
>
> Third: The defendant did so knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represented the proceeds of some form of unlawful activity; and
>
> Fourth: The defendant knew that the transportation, transmission, or transfer was designed, in whole or in part, to conceal or disguise the nature, the location, the source, the ownership or the control of the proceeds of fraud and related activity in connection with computers.

The elements of 18 U.S.C. § 1957 include the following:[8]

> First: That the defendant knowingly engaged or attempted to engage in a monetary transaction;
>
> Second: That the monetary transaction was of a value greater than $10,000;
>
> Third: That the monetary transaction involved criminally derived property;
>
> Fourth: That criminally derived property was derived from specified unlawful activity;
>
> Fifth: That the defendant knew that the monetary transaction involved criminally derived property; and
>
> Sixth: That the monetary transaction took place within the United States.

[7] As noted, there is no Fifth Circuit Pattern Jury Instruction. The statute is included above and the Seventh Circuit Pattern Instruction is included herein.

[8] Fifth Circuit Pattern Instruction 2.77 (5th 2019).

STIPULATED FACTS

1. Yaroslav Vasinskyi admits and agrees that starting in or about March 2019, and continuing to in or about August 2021, within the Northern District of Texas and elsewhere, he knowingly and willfully combined, conspired, confederated, and agreed with others to commit offenses against the United States—that is, 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 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).

2. Yaroslav Vasinskyi further admits and agrees that on the specific dates alleged in the indictment, within the Northern District of Texas and elsewhere, he and others 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 of the victims identified as Company A through Company I in the indictment, in violation of 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B), and 2.

3. Yaroslav Vasinskyi also admits and agrees that starting in or about March 2019, and continuing on or about August 2021, within the Northern District of Texas, and elsewhere, he and others did knowingly combine, conspire, confederate, and agree 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 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. Such conduct was all in violation of 18 U.S.C. § 1956(h).

4. More specifically, between in or about March 2019 and August 2021, the defendant and others engaged in a ransomware and money laundering conspiracy using the ransomware variant known as Sodinokibi or REvil. Generally, the conspiracy was accomplished in the following manner: Conspirators authored Sodinokibi ransomware, which was designed to encrypt data on victims' computers. Using the Sodinokibi ransomware, the defendant and other conspirators infected victims' computers in various ways, including by (1) deploying phishing emails to collect the recipients' credentials and to deliver malware; (2) using compromised remote desktop credentials; and (3) exploiting security vulnerabilities in software code and operating systems. The defendant and other conspirators then obtained persistent remote access to the victims' compromised networks and used malware to gain further access and control of other computers in the victims' networks. The defendant and other conspirators then deployed Sodinokibi ransomware on the victims' networks. Beginning in or about January 2020, members of the conspiracy began exfiltrating the victims' data prior to deploying the Sodinokibi ransomware. Once exfiltrated, members of the conspiracy posted portions of the victims' data on a blog to (1) prove they had taken the victims' data, and (2) to threaten publication of all the victims' data if ransoms were not paid.

5. Through the deployment of Sodinokibi ransomware, the defendant and other conspirators damaged and encrypted the files on the victims' computers. As a part of the conspiracy, the defendant and 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. 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. In the event a victim paid the ransom amount, the defendant and conspirators provided the decryption key to the victim, and the victim was then able to access its files. In the event a victim did not pay the ransom, the conspirators typically posted the victim's exfiltrated data or claimed that they sold the exfiltrated data to third parties.

6. In the cybercrime underground and as a part of his involvement in the Sodinokibi ransomware attacks, the defendant used the moniker "Rabotnik." During the course of his involvement in the charged conspiracies, the defendant conducted approximately 2,500 attacks on computers in the United States between May 2019 and August 2021. The ransoms demanded as a result of those attacks totaled in excess of $700 million, and the ransoms paid by victims for those attacks totaled approximately $2.3 million. The ransoms were paid using via virtual currency, e.g. Bitcoin or Monero. That is, the victims caused the money to be transferred electronically from a location in the United States to cryptocurrency accounts (wallets) held by individuals located outside the United States. As a part of the conspiracy, cryptocurrency exchangers and mixing services were used to conceal and disguise the nature, the location, the source, the ownership, and the control of the proceeds.

7. The Sodinokibi ransomware attacks conducted by the defendant included, but were not limited to the following:

a. On or about May 21, 2019, against Company A, an entity located in Braintree, Massachusetts.

b. On or about July 2, 2021, against Kaseya, referred to as Company B in the indictment, a business located in Miami, Florida.

c. On or about July 2, 2021, against Company C, a business located in Yonkers, New York.

d. On or about July 2, 2021, against Company D, a financial institution located in Dallas, Texas, which was located in the Northern District of Texas.

e. On or about July 2, 2021, against Company E, a business located in Addison, Texas, which was located in the Northern District of Texas.

f. On or about July 2, 2021, against Company F, a business located in Dallas, Texas, which was located in the Eastern District of Texas.

g. On or about July 2, 2021, against Company G, a business located in Stamford, Connecticut.

h. On or about July 2, 2021, against Company H, a business located in La Plata, Maryland.

i. On or about July 2, 2021, against Company I, a business located in Fairfield, New Jersey.

j. On or about July 2, 2021, against Company J, a business located in Tempe, Arizona.

As a result of each of the above attacks conducted by the defendant, the offense caused

loss to persons during a 1-year period affecting protected computers aggregating at least $5,000 in value, and/or caused damage affecting 10 or more protected computers during a 1-year period. Following his arrest, the defendant was extradited to the United States and first brought to the Northern District of Texas.

8. The defendant agrees that he committed all the essential elements of the offenses. This factual resume is not intended to be a complete accounting of all the facts and events related to the offense charged in this case. The limited purpose of this statement of facts is to demonstrate that a factual basis exists to support the defendant's guilty plea to Counts One through Eleven of the indictment.

AGREED TO AND STIPULATED on this 29th day of ~~March~~ July 2022.

Yaroslav Vasinskyi

YAROSLAV VASINSKYI
Defendant

SIMON KABLAN
Attorney for Defendant

N/A

STEPHEN GREEN
Attorney for Defendant

CHAD E. MEACHAM
UNITED STATES ATTORNEY

TIFFANY H. EGGERS
Assistant United States Attorney
Florida Bar Number 0193968
1100 Commerce Street, 3rd Floor
Dallas, Texas 75242
Tel: 214-659-8600
Fax: 214-659-8605
Email: Tiffany.Eggers@usdoj.gov