

UNDER SEAL

FILED 11 AUG '21 15:39 USDC-ORP

**UNITED STATES DISTRICT COURT
DISTRICT OF OREGON
PORTLAND DIVISION**

UNITED STATES OF AMERICA

3:20-cr-00237-JO

v.

SECOND SUPERSEDING INDICTMENT

18 U.S.C. § 1956(h)

Forfeiture Allegation

UNDER SEAL

DENIS MIHAQLOVIC DUBNIKOV,

, and

Defendants.

THE GRAND JURY CHARGES:

1. [REDACTED]

hereinafter referred to as defendant [REDACTED]

2. [REDACTED]

hereinafter referred to as

defendant [REDACTED]

///

Second Superseding Indictment

Page 1

3. [REDACTED], hereinafter referred to as defendant [REDACTED].

4. [REDACTED], hereinafter referred to as defendant [REDACTED].

5. [REDACTED], hereinafter referred to as defendant [REDACTED].

6. [REDACTED], hereinafter referred to as defendant [REDACTED].

7. **DENIS MIHAQLOVIC DUBNIKOV** is a citizen of Russia, hereinafter referred to as defendant **DUBNIKOV**.

8. [REDACTED], hereinafter referred to as defendant [REDACTED].

9. [REDACTED], hereinafter referred to as defendant [REDACTED].

10. [REDACTED], hereinafter referred to as defendant [REDACTED].

11. [REDACTED], hereinafter referred to as defendant [REDACTED].

12. [REDACTED], hereinafter referred to as defendant [REDACTED].

13. [REDACTED]
hereinafter referred to as defendant [REDACTED].

///

14. [REDACTED] hereinafter referred to as defendant
[REDACTED]

Ransomware Scheme

15. Ransomware is a type of malicious software designed to encrypt data on a victim's computer or network that prevents a victim from accessing those files until a ransom is paid.

16. The Ryuk ransomware, hereinafter referred to as Ryuk, was first used against a victim in or around August 2018. When executed on a computer or network, Ryuk attempts to delete any backup files present on the computer or network and then begins to encrypt files. Files on any storage drives contained within or physically connected to the computer, including any accessible over a network connection, are subject to being encrypted by Ryuk. A "ransom note" is placed onto the computer system when files are encrypted, providing email addresses, typically a foreign, web-based email provider, that the victims could use to contact the individuals using Ryuk, hereinafter referred to as the Ryuk actors. The Ryuk actors also provide a bitcoin wallet address that victims could use to pay a ransom to have their files decrypted.¹

17. While the ransom notes changed over time, early ransom notes were as follows:

Gentlemen!

Your business is at serious risk.

There is a significant hole in the security system of your company.

We've easily penetrated your network.

You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks.

They can damage all your important data just for fun.

Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.

No one can help you to restore files without our special decoder.

¹ Bitcoin is a form of decentralized, convertible digital or cryptocurrency that exists through the use of an online, decentralized ledger system. Bitcoin is just one of several forms of digital currency and has the largest market share of any decentralized digital currency.

*Photorec, RannohDecryptor etc. repair tools
are useless and can destroy your files irreversibly.*

*If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).*

*You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.*

*You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC
Nothing personal just business*

*As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security
and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.*

Attention! One more time!

*Do not rename encrypted files.
Do not try to decrypt your data using third party software.*

*P.S. Remember, we are not scammers.
We don't need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty – decrypted samples.*

Contact emails

[OMITTED]

or

[OMITTED]

*BTC wallet:
[OMITTED]*

No system is safe

///

18. The Ryuk actors attacked thousands of victims worldwide, including thousands in the United States and multiple in Oregon. Victims come from a variety of sectors, including private industry, state and local municipalities, local school districts, critical infrastructure, and hospitals and other healthcare services and providers. Ryuk attacks have severely disrupted these entities' abilities to function by restricting access to data and impacting communications. Ryuk victims have paid approximately \$150 million in ransoms to recover critical files.

19. Defendants and other unindicted co-conspirators laundered ransom payments through a series of financial transactions, including crypto and fiat currency-based transactions, to conceal and disguise the nature, source, location, ownership, and control of the unlawful proceeds.² Aside from personal enrichment, they used the ransom payments to, among other things, facilitate or promote the criminal ransomware activity.

Laundering of Ransom Payments

20. As noted above, the Ryuk actors directed victims to pay in bitcoin and provided the victims with a bitcoin wallet address (a bitcoin public key) to which to make the ransom payments.

21. Bitcoin and other cryptocurrencies may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. It can be exchanged directly from person to person, through a cryptocurrency exchange, or through other intermediaries. Bitcoin, and most cryptocurrencies, has a "blockchain," a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.

² Fiat currency is currency established by government regulation or law, *e.g.*, U.S. dollars, Euros, Russian Rubles, or Chinese Renminbi.

22. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key.

23. The public key, hereinafter referred to as the “address,” is represented as a case-sensitive string of letters and numbers. A user of cryptocurrency provides the address to others to receive cryptocurrency.

24. The private key is a password that is not shared publicly. A person who possesses the private key, possesses and controls the cryptocurrency wallet and the cryptocurrency in that wallet.

25. Users of cryptocurrency store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device (“hardware wallet”), downloaded on a PC or laptop (“desktop wallet”), with an Internet-based cloud storage provider (“online wallet”), or as a mobile application on a smartphone or tablet (“mobile wallet”) (hereinafter collectively referred to as “private wallets”). Private wallets are generally anonymous and conceal the identity of the individual(s) in control of the wallets as well as the location, ownership, and control of the wallets and digital currency in the wallets.

26. Cryptocurrency exchanges, typically companies, offer a variety of services to customers including online wallets and, typically for a fee, the ability to purchase different forms of cryptocurrency and to exchange cryptocurrency for other forms of cryptocurrency or a variety of fiat currency. Customers may open an account with an exchange, hereinafter referred to as an “exchange account,” and many exchanges maintain customer information.

27. Cryptocurrency's value, like bitcoin, relative to fiat currency like the United States dollar, fluctuates over time. For example, bitcoin traded for approximately \$6,322.69 on August 12, 2018, the date the first documented Ryuk ransom was requested, and for approximately \$9,204.30 on July 15, 2020, and for approximately \$45,517.80 on August 10, 2021.

28. Not every cryptocurrency fluctuates in value against the United States dollar. For example, Tether, a "stablecoin," attempts to keep its valuation consistent with a fiat currency like the United States dollar. As a stablecoin, Tether avoids the volatility of decentralized digital currency like bitcoin.

29. The Ryuk actors used anonymous private wallets in their ransom notes, allowing them immediately to conceal the nature, location, source, ownership, and control of the ransom payments.

30. After receiving the ransom payments, the Ryuk actors, defendants, and others involved in the scheme engaged in various financial transactions, including international financial transactions, to conceal the nature, source, location, ownership, and control of the ransom proceeds. They also used proceeds from the ransom payments to facilitate or promote the specified unlawful activities, that is, Computer Hacking in violation of 18 U.S.C. § 1030, Wire Fraud in violation of 18 U.S.C. § 1343, and Conspiracy to Commit Wire Fraud in violation of 18 U.S.C. § 1349 (hereinafter the "Specified Unlawful Activities") by paying individuals to develop and deploy ransomware, to identify victims for ransomware attacks, to carry out ransomware attacks, to maintain infrastructure, communication facilities, and similar needs in order to carry out ransomware attacks and extort victims of ransomware attacks, to launder ransom payments, and to fulfill other aspects of the Specified Unlawful Activities.

COUNT 1
(Conspiracy to Commit the Laundering of Monetary Instruments)
(18 U.S.C. § 1956(h))

31. All prior paragraphs of the Second Superseding Indictment are incorporated herein.

32. Beginning on an unknown date but no later than in or about August 2018, and continuing through the date of this Second Superseding Indictment, in the District of Oregon and elsewhere, defendants [REDACTED],
[REDACTED] DUBNIKOV, [REDACTED],
[REDACTED], and [REDACTED], and others, known and unknown to the grand jury, did knowingly combine, conspire, confederate and agree to:

a. knowingly conduct and attempt to conduct a financial transaction affecting interstate and foreign commerce which involved the proceeds of Specified Unlawful Activities with the intent to promote the carrying on of the Specified Unlawful Activities and that while conducting and attempting to conduct such financial transaction knew that the property involved in the financial transaction represented the proceeds of some form of unlawful activity in violation of 18 U.S.C. § 1956(a)(1)(A)(i);

b. knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce knowing the transactions represented the proceeds of some form of unlawful activity and were designed in whole or in part to conceal and disguise the nature, location, source, ownership and control of the proceeds of the Specified Unlawful Activities in violation of 18 U.S.C. § 1956(a)(1)(B)(i);

c. knowingly transport, transmit, and transfer, or attempt to transport, transmit, and transfer, monetary instruments or funds from the United States to or

through a place outside of the United States, or to the United States from or through a place outside of the United States knowing the monetary instrument or funds represented the proceeds of some form of unlawful activity and knowing the international movement was designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of the Specified Unlawful Activities in violation of 18 U.S.C. § 1956(a)(2)(B)(i); and

d. knowingly engage and attempt to engage in monetary transactions, by, through, and to a financial institution, in and affecting interstate and foreign commerce, in criminally derived property in amounts greater than \$10,000 and was derived from the Specified Unlawful Activities in violation of 18 U.S.C. § 1957.

Manner and Means

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

34. Defendants and other unindicted co-conspirators laundered the proceeds of the ransom payments using a variety of financial transactions involving private wallets, exchanges and exchange accounts, and several cryptocurrencies and fiat currencies.

35. Defendants and others involved in the laundering took numerous steps to conceal and disguise the nature, location, source, ownership, and control of the proceeds, including using numerous private wallets, splitting proceeds among numerous wallets and exchange accounts, making circular transfers of proceeds in various amounts, transferring proceeds to exchange accounts in the names of various individuals, converting proceeds from bitcoin to other cryptocurrencies, converting proceeds from cryptocurrency into fiat currency, conducting foreign

financial transactions, and regularly changing methods and individuals involved in the laundering activities.

36. Although defendants and others involved in the conspiracy used different methods at times to avoid detection, ransom payments were typically laundered as follows. After victims paid ransoms in bitcoin to private wallets, defendants and other unindicted co-conspirators involved in the scheme split the ransom payments into smaller amounts, transferring them in varying amounts to numerous other private wallets. Generally, at this stage, defendants and others used private wallets to conceal the nature, location, source, ownership, and control of the ransom proceeds. Defendants and other unindicted co-conspirators used hundreds of private wallets with thousands of associated public keys to conduct these transactions.

37. Next, defendants and other unindicted co-conspirators transferred some of the bitcoin from private wallets into exchange accounts.

38. Once the bitcoin was transferred to an exchange account, defendants and other unindicted co-conspirators took additional steps to conceal and disguise the nature, location, source, ownership, and control of the proceeds, including:

- a. Exchanging the bitcoin for Tether, for another cryptocurrency, or for fiat currency;
- b. After exchanging the bitcoin for Tether or another cryptocurrency, sending ransom proceeds (now in the form of Tether or another cryptocurrency) to other co-conspirators' accounts at various cryptocurrency exchanges, where other co-conspirators exchanged the Tether (or another cryptocurrency) for fiat currency, typically Chinese

Renminbi, using that cryptocurrency exchange's "over the counter" service to sell Tether (or another cryptocurrency) for fiat currency;³


c. After exchanging the ransom payments in the form of Tether (or another cryptocurrency) for fiat currency, moving it into accounts at financial institutions outside the United States; or



40. Defendants and other unindicted co-conspirators engaged in financial transactions with the proceeds of the criminal scheme in order to promote the criminal activity, such as paying for services and infrastructure used to maintain and support the Specified Unlawful Activities.

The Named Defendants

41. Between in or about August 2018 through in or about February 2019, defendant

 laundered more than \$2.5 million in Ryuk ransom proceeds.

42. Between in or about March 2019 through in or about March 2021, defendant

 laundered more than \$5 million in Ryuk ransom proceeds.

///

³ Some cryptocurrency exchanges offer an over-the-counter trading service that allows customers to trade cryptocurrency for fiat currency directly—that is, two customers agree on a price and transfer the assets between themselves.

43. Between in or about March 2019 through in or about June 2019, defendant [REDACTED] laundered more than \$2 million in Ryuk ransom proceeds.

44. Between in or about July 2019 through in or about March 2020, defendant [REDACTED] laundered more than \$20 million in Ryuk ransom proceeds.

45. In or about March 2019, defendant [REDACTED] laundered more than \$600,000 in Ryuk ransom proceeds.

46. Between in or about March 2019 through in or about July 2019, defendant [REDACTED] laundered more than \$1 million in Ryuk ransom proceeds.

47. In or about July 2019, defendant **DUBNIKOV** laundered more than \$400,000 in Ryuk ransom proceeds.

48. In or about October 2018, defendant [REDACTED] laundered more than \$60,000 in Ryuk ransom proceeds.

49. In or about May 2019, defendant [REDACTED] laundered more than \$350,000 in Ryuk ransom proceeds.

50. Between in or about April 2019 through in or about June 2019, defendant [REDACTED] laundered more than \$850,000 in Ryuk ransom proceeds.

51. Between in or about June 2019 through in or about August 2019, defendant [REDACTED] laundered more than \$2.2 million in Ryuk ransom proceeds.

52. Between in or about March 2019 through in or about December 2019, defendant [REDACTED] laundered more than \$1.1 million in Ryuk ransom proceeds.

53. Between in or about August 2018 through in or about September 2020, defendant [REDACTED] laundered more than \$100,000 in Ryuk ransom proceeds.

///

54. Between in or about February 2020 through in or about July 2021, defendant [REDACTED] laundered more than \$35 million in Ryuk ransom proceeds.

All in violation of 18 U.S.C. § 1956(h).

FORFEITURE ALLEGATION

55. Upon conviction of the offense alleged in Count 1 of this Second Superseding Indictment, defendants shall forfeit to the United States pursuant to 18 U.S.C. § 982(a)(1), all property, real and personal, involved in the money laundering offenses and all property traceable to such property.

SUBSTITUTE ASSETS

56. If any forfeitable property, as a result of any act or omission of the defendants:

- (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; 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), to seek forfeiture of any other property of said defendants up to the value of the forfeitable property described above.

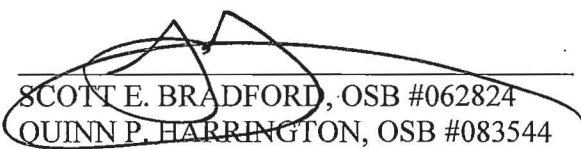
Dated: August 11, 2021.

A TRUE BILL


OFFICIATING FOREPERSON

Presented by:

SCOTT ERIK ASPHAUG
Acting United States Attorney


SCOTT E. BRADFORD, OSB #062824
QUINN P. HARRINGTON, OSB #083544
WILLIAM M. NARUS, CAB #243633
Assistant United States Attorneys