UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

UNITED STATES OF AMERICA	)	
	)	NO. 3:23-00088
	)	
	)	18 U.S.C. § 371
	)	18 U.S.C. § 1030(a)(2)(C)
v.	)	18 U.S.C. § 1030(a)(5)(A)
	)	18 U.S.C. § 1030(a)(7)(C)
	)	18 U.S.C. § 1343
	)	18 U.S.C. § 1349
OLEKSII OLEKSIYOVYCH LYTVYNENKO	)	
a/k/a ALEXSEY ALEXSEEVICH LITVINENKO	)	**FILED UNDER SEAL**

INDICTMENT

THE GRAND JURY CHARGES:

At times relevant to this Indictment:

COUNT ONE

BACKGROUND

1. **OLEKSII OLEKSIYOVYCH LYTVYNENKO, a/k/a ALEXSEY ALEXSEEVICH LITVINENKO,** and other persons known and unknown to the grand jury, conspired to attack businesses, nonprofits, and governments in the United States and around the world using malicious software known as "Conti," a type of ransomware.

2. In furtherance of the scheme, the conspirators hacked into victims' computer networks and copied the victims' data to the conspirators' own computers. The conspirators then encrypted the victims' data, which prevented the victims from accessing their own files. The conspirators typically then demanded a ransom to restore the victims' access to their files and to

prevent the conspirators from publicly disclosing the hack and releasing the victims' stolen data to the internet.

3. Different conspirators had different roles in the conspiracy, including: (1) developing Conti ransomware; (2) "crypting" Conti ransomware so that it would evade detection by anti-virus programs; (3) managing teams of hackers; (4) gaining initial access to victims' networks; (5) deploying Conti ransomware on victims' networks; and (6) negotiating with victims.

4. **OLEKSII OLEKSIYOVYCH LYTVYNENKO a/k/a ALEXSEY ALEXSEEVICH LITVINENKO** and his co-conspirators have claimed attacks on more than nine hundred victims worldwide, including many in the United States. In particular, they have attacked:

a. Victim 1: a government entity located in the Middle District of Tennessee;

b. Victim 2: a business located in the Middle District of Tennessee; and

c. Victim 3: a business located in the Middle District of Tennessee.

RELEVANT TERMS

5. A "network" was a group of two or more computers linked together.

6. A "server" was a type of computer or device on a network that managed network resources and/or provided services for other computers connected to it via a network or the internet. Servers could be located thousands of miles from other computers on the network.

7. "Encryption" was the translation of data into secret code. To access encrypted data, a user needed to have access to a password (known as a "decryption key" or "decrypter") that enabled the user to decrypt it.

8. "Ransomware" was a type of malicious software which infected a computer or network and encrypted some or all of the data stored there. Ransomware users typically demanded

that the owner of the encrypted computer or network pay a ransom for a decryption key, often in digital currency.

9. "Cryptocurrencies," such as Bitcoin, were electronically sourced units of value that existed on the internet. Cryptocurrencies were generated and tracked through computer software in a peer-to-peer network, rather than issued from a government or other entity. Users of cryptocurrencies sent units of value to and from "addresses," which were unique strings of numbers and letters that functioned like a public account number. Cryptocurrency transactions were recorded on a publicly available, distributed ledger, often referred to as a "blockchain." Cryptocurrency transactions generally did not disclose information about the participating parties, as transactions usually required only the addresses and the online usernames of the parties.

10. "Tor" was a computer network designed to facilitate anonymous communication over the internet. Typically, user activities on the internet could be attributed to the user via Internet Protocol ("IP") addresses assigned by an internet service provider. The Tor network routed a user's communications through a globally distributed network of relay computers or proxies (the "Tor network"), which typically prevented identification of users by IP address.

THE CONSPIRACY

11. Beginning no later than in or about 2020 and continuing thereafter until at least in or about June 2022, in the Middle District of Tennessee and elsewhere, **OLEKSII OLEKSIYOVYCH LYTVYNENKO, a/k/a ALEXSEY ALEXSEEVICH LITVINENKO,** and others known and unknown to the Grand Jury, did knowingly and intentionally conspire, confederate, and agree to commit offenses against the United States, that is:

a. to intentionally access a computer without authorization, and thereby obtain information from a protected computer, and to commit the offense for

purposes of private financial gain, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i);

b. 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 one or more persons during a 1-year period aggregating at least $5,000.00 in value, and cause damage affecting 10 or more protected computers during a 1-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B); and

c. to, with intent to extort from any person any money or 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 Title 18, United States Code, Sections 1030(a)(7)(C) and 1030(c)(3)(A).

Objects of the Conspiracy

12. The purpose of the conspiracy was for **OLEKSII OLEKSIYOVYCH LYTVYNENKO, a/k/a ALEXSEY ALEXSEEVICH LITVINENKO,** and his co-conspirators (hereinafter "Conti conspirators") to enrich themselves by:

a. developing Conti ransomware;

b. identifying vulnerabilities in victims' networks;

c. exploiting those vulnerabilities to access victims' computers without authorization;

d. stealing victims' data;

e. installing and executing Conti ransomware on victims' computers, resulting in the encryption of the data on those computers;

f. extorting victims by demanding a cryptocurrency ransom in exchange for:

(i) a decryption key for the encrypted data;

(ii) a promise not to publicize the breach of victims' networks on a Tor website operated by Conti conspirators; and

(iii) a promise not to publicly release victims' stolen data on the same Tor website; and

g. collecting ransom payments from victims and dividing those payments among Conti conspirators.

Manner and Means of the Conspiracy

13. The manner and means used to accomplish the conspiracy's objectives included the following:

a. Conti conspirators developed Conti ransomware no later than 2020. Since that time, the Conti conspirators have released at least three different versions of the Conti ransomware.

b. Conti conspirators identified potential victims and searched for vulnerabilities in victims' networks.

c. After identifying those vulnerabilities, Conti conspirators hacked into (i.e., accessed without authorization) the networks of victims.

d. Once inside victims' networks, Conti conspirators sought to obtain persistent remote access to the networks, move laterally (i.e., access other

systems within the computer or network), and escalate privileges (i.e., gain greater authority over the computer or network).

e. After gaining sufficient privileges to the victims' networks, Conti conspirators stole victim data and deployed Conti ransomware.

f. As part of the deployment of Conti ransomware, the victims' files were encrypted and the ransomware left a ransom note in the form of a text file on the victims' computers. Many versions of the note stated, in part, "if you don't [know Conti] – just 'google it.'" The note typically also demanded that the victims access a Tor website address for "further instructions."

g. That Tor website directed victims to upload their ransom note, which permitted them to engage in text negotiations with Conti conspirators. Conti conspirators who negotiated with victims typically provided victims with a cryptocurrency address for the payment of the demanded ransom.

h. Beginning in or about December 2020, if victims did not quickly engage in ransom negotiations, Conti conspirators began publishing portions of the victims' data to a Tor website, and threatened to publish more if the victims did not pay the ransom.

i. Victims who paid the ransom typically received a decryption key and their stolen files were not further published. Conti conspirators typically published the data of victims who did not pay the ransom.

Overt Acts

14. In furtherance of the conspiracy, and to achieve the goals and objectives of the conspiracy, Conti conspirators committed and caused to be committed the following overt acts, among others, in the Middle District of Tennessee and elsewhere:

a. Beginning no later than in or about 2020, Conti conspirators developed Conti ransomware.

b. On or about July 28, 2020, Conti conspirators deployed their ransomware on the network of Victim 1, a government entity in the Middle District of Tennessee, and encrypted its network—including its Sheriff's Department's computers—without authorization.

c. Shortly after the attack on Victim 1, Conti conspirators also moved laterally and encrypted the related systems of local emergency medical services and another local police department.

d. Conti conspirators ultimately extorted Victim 1 (which was insured) into paying a ransom of approximately $174,000 in Bitcoin to Conti conspirators in exchange for a decryption key and to avoid publication of Victim 1's data.

e. On or about September 9, 2021, Conti conspirators deployed their ransomware on the network of Victim 2, a business located in the Middle District of Tennessee, and encrypted its network, without authorization.

f. Conti conspirators initially demanded $950,000 from Victim 2.

g. On Conti's Tor website, after Victim 2 told Conti conspirators, "I've done everything I can to collect us [sic] much money as possible . . . I've been

begging everyone for help," a Conti conspirator responded, "Stop telling tales, you're a bad negotiator. You have a choice to pay or be published."

h. Conti conspirators ultimately extorted Victim 2 into paying a ransom of approximately $460,000 in Bitcoin to Conti conspirators in exchange for a decryption key and to avoid publication of Victim 2's data.

i. On or about January 29, 2022, Conti conspirators deployed their ransomware on the network of Victim 3, also a business in the Middle District of Tennessee, and encrypted its network, without authorization.

j. When Victim 3 contacted Conti through the group's Tor website, Conti conspirators demanded a ransom of $3,000,000.

k. When Victim 3 rejected the ransom demand, Conti conspirators published the data they stole from Victim 3, including annual audit and 401(k) files.

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

COUNT TWO

THE GRAND JURY FURTHER CHARGES:

15. The Grand Jury re-alleges and incorporates by reference Paragraphs 1 through 10, 12, and 13 of Count One, as if fully set forth herein.

16. Beginning no later than 2020 and continuing thereafter until at least in or about June 2022, in the Middle District of Tennessee and elsewhere, **OLEKSII OLEKSIYOVYCH LYTVYNENKO, a/k/a ALEXSEY ALEXSEEVICH LITVINENKO,** and others known and unknown to the Grand Jury, did knowingly and willfully combine, confederate and agree with each other to devise and intend to devise a scheme and artifice to defraud ransomware victims, and to obtain money and property by means of materially false and fraudulent pretenses, representations

and promises, and for the purpose of executing the scheme described above, cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, and signals, in violation of Title 18, United States Code, Section 1343.

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

FORFEITURE ALLEGATIONS

17. The allegations contained in this Indictment are incorporated and re-alleged as if fully set forth herein in support of this forfeiture allegation.

18. Upon conviction of Count One or Two, **OLEKSII OLEKSIYOVYCH LYTVYNENKO, a/k/a ALEXSEY ALEXSEEVICH LITVINENKO,** shall forfeit to the United States of America pursuant to Title 18, United States Code, Section 981(a)(1)(C) by Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the offense, including but not limited to a money judgment representing the amount of the proceeds of the offense.

19. Upon conviction of Count One, **OLEKSII OLEKSIYOVYCH LYTVYNENKO, a/k/a ALEXSEY ALEXSEEVICH LITVINENKO,** shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of the offense, including but not limited to, a money judgment representing the proceeds of such offense; and pursuant to Title 18, United States Code, Section 1030(i), all right, title, and interest in any personal property that was used or intended to be used to commit or to facilitate the commission of the offense.

20. If through any acts or omission by **OLEKSII OLEKSIYOVYCH LYTVYNENKO, a/k/a ALEXSEY ALEXSEEVICH LITVINENKO,** any or all of the property

described in paragraphs 18 and 19, above:

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;

the United States of America shall be entitled to forfeiture of substitute property of the Defendant up to the value of the above-described forfeitable property, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b) and 1030(i), and Title 28, United States Code, Section 2461(c).

A TRUE BILL

[redacted]

GRAND JURY FOREPERSON

HENRY C. LEVENTIS
UNITED STATES ATTORNEY

TAYLOR J. PHILLIPS
ASSISTANT UNITED STATES ATTORNEY

SONIA V. JIMENEZ
RYAN K.J. DICKEY
TRIAL ATTORNEYS

CRIMINAL COVER SHEET
MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

Indictment (x)
Complaint ( )
Information ( )
Misdemeanor ( )
Felony (x)
Juvenile ( )

County of Offense: Davidson
AUSA's NAME: Taylor J. Phillips

Reviewed by AUSA: TJP
(Initials)

OLEKSII OLEKSIYOVYCH LYTVYNENKO
Defendant's Full Name

Ireland
Defendant's Address

Interpreter Needed? __X__ Yes ___ No

If Yes, what language? Ukrainian

Defendant's Attorney

COUNTS	TITLE/SECTION	OFFENSE CHARGED	MAX. PRISON (plus any mandatory minimums)	MAX. FINE
1	**18 U.S.C. § 371**	**Conspiracy to Violate the CFAA**	**5 years**	**$250,000**
2	**18 U.S.C. § 1349**	**Conspiracy to Commit Fraud**	**20 years**	**$250,000**
		Forfeiture		

*Pursuant to 18 U.S.C. §3014, the defendant may be subject to an additional $5000 special assessment.

Is the defendant currently in custody? ( ) Yes (x) No
If Yes, State or Federal? _____
Writ requested ( )

Has a complaint been filed? ( ) Yes (x) No
If Yes: Name of Magistrate Judge _____ Case No.: _____
Was the defendant arrested on the complaint? ( ) Yes (X) No

Has a search warrant been issued? (X) Yes () No
If Yes: Name of Magistrate Judge Alistair Newbern Case No.: 21-mj-4134

Was bond set by Magistrate/District Judge: ( ) Yes ( ) No (x) Not Applicable Amount of bond: _____

Is this a Rule 20? ( ) Yes (x) No To/from what district? _____
Is this a Rule 40? ( ) Yes (x) No To/from what district? _____

Estimated trial time: 10 days

The Clerk will issue a Warrant

Detention requested: Yes (X) No ( ) Recommended conditions of release: _____

(Revised January 2019)