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 24 PM 5:03

DEPUTY CLERK

UNITED STATES OF AMERICA

V.

Yevgeniy Igorevich Polyanin (01)
a/k/a Evgeniy Igorevich Polyanin
a/k/a Evgeniy Polyanin
a/k/a LK4D4
a/k/a Damnating
a/k/a Damn2life
a/k/a Noolleds
a/k/a Antunpitre
a/k/a Affiliate 23

CRIMINAL NO.

FILED UNDER SEAL

3-21CR0393-B

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 programing 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. Company A was a business located in Weatherford, Texas which was located in the Northern District of Texas.

17. Company B was a business located in Rockwall, Texas which was located in the Northern District of Texas.

18. Government Entity C was an entity located in Borger, Texas which was located in the Northern District of Texas.

19. Government Entity D was an entity located in Graham, Texas which was located in the Northern District of Texas.

20. Government Entity E was an entity located in Kaufman, Texas which was located in the Northern District of Texas.

21. Government Entity F was an entity located in Kaufman, Texas which was located in the Northern District of Texas.

22. Government Entity G was an entity located in Keene, Texas which was located in the Northern District of Texas.

23. Government Entity H was an entity located in the Northern District of Texas.

24. Government Entity I was an entity located in Brownfield, Texas which was located in the Northern District of Texas.

25. Government Entity J was an entity located in Vernon, Texas which was located in the Northern District of Texas.

26. Government Entity K was an entity located in Venus, Texas which was located in the Northern District of Texas.

27. Government Entity L was an entity located in Wilmer, Texas which was located in the Northern District of Texas.

28. Government Entity M was an entity located in Kaufman, Texas which was located in the Northern District of Texas.

29. Government Entity N was an entity located in Palmer, Texas which was located in the Northern District of Texas.

30. Government Entity O was an entity located in Venus, Texas which was located in the Northern District of Texas.

31. Defendant **Yevgeniy Igorevich Polyanin** was a citizen of Russia. **Polyanin** used various online monikers including, Evgeniy Igorevich Polyanin, Evgeniy Polyanin, LK4D4, Damnating, Damn2life, Noolleds, Antunpitre, and Affiliate 23.

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)]

32. Paragraphs 1 through 31 of this indictment are re-alleged and incorporated by reference as though fully set forth herein.

33. From on or about March 1, 2019, through on or about August 24, 2021, in the Northern District of Texas and elsewhere, defendant **Yevgeniy Igorevich Polyanin** 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, cause damage affecting 10 or more protected computers during a 1-year period, and cause damage affecting a computer used by and for an entity of the United States Government in furtherance of the administration of justice 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

34. It was the purpose of the conspiracy for defendant **Yevgeniy Igorevich Polyanin** 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

35. The manner and means by which defendant **Yevgeniy Igorevich Polyanin** 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

36. In furtherance of the conspiracy and to affect its unlawful objects, defendant **Yevgeniy Igorevich Polyanin** 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 August 5, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators accessed the internal computer networks of Company A without authorization.

b. On or about August 5, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators deployed Sodinokibi ransomware on Company A's computers thereby encrypting Company A's computers.

c. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators accessed the internal computer networks of Company B without authorization and caused damage.

d. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators accessed the internal computer networks of Company B's clients without authorization.

e. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators deployed Sodinokibi ransomware on Company B's clients thereby encrypting Company B's clients' computers.

f. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators accessed the internal computer networks of Government Entity C without authorization.

g. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators deployed Sodinokibi ransomware on Government Entity C's computers, thereby encrypting Government Entity C's computers.

h. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators accessed the internal computer networks of Government Entity D without authorization.

i. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators deployed Sodinokibi ransomware on Government Entity D's computers, thereby encrypting Government Entity D's computers.

j. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators accessed the internal computer networks of Government Entity E without authorization.

k. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators deployed Sodinokibi ransomware on Government Entity E's computers, thereby encrypting Government Entity E's computers.

l. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators accessed the internal computer networks of Government Entity F without authorization.

m. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators deployed Sodinokibi ransomware on Government Entity F's computers, thereby encrypting Government Entity F's computers.

n. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators accessed the internal computer networks of Government Entity G without authorization.

o. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators deployed Sodinokibi ransomware on Government Entity G's computers, thereby encrypting Government Entity G's computers.

p. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators accessed the internal computer networks of Government Entity H without authorization.

q. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators deployed Sodinokibi ransomware on Government Entity H's computers, thereby encrypting Government Entity H's computers.

r. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators accessed the internal computer networks of Government Entity I without authorization.

s. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators deployed Sodinokibi ransomware on Government Entity I's computers, thereby encrypting Government Entity I's computers.

t. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators accessed the internal computer networks of Government Entity J without authorization.

u. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators deployed Sodinokibi ransomware on Government Entity J's computers, thereby encrypting Government Entity J's computers.

v. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators accessed the internal computer networks of Government Entity K without authorization.

w. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators deployed Sodinokibi ransomware on Government Entity K's computers, thereby encrypting Government Entity K's computers.

x. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators accessed the internal computer networks of Government Entity L without authorization.

y. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators deployed Sodinokibi ransomware on Government Entity L's computers, thereby encrypting Government Entity L's computers.

z. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators accessed the internal computer networks of Government Entity M without authorization.

aa. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators deployed Sodinokibi ransomware on Government Entity M's computers, thereby encrypting Government Entity M's computers.

bb. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators accessed the internal computer networks of Government Entity N without authorization.

cc. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators deployed Sodinokibi ransomware on Government Entity N's computers, thereby encrypting Government Entity N's computers.

dd. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators accessed the internal computer networks of Government Entity O without authorization.

ee. On or about August 16, 2019, defendant **Yevgeniy Igorevich Polyanin** and other conspirators deployed Sodinokibi ransomware on Government Entity O's computers, thereby encrypting Government Entity O's 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 Thirteen
Intentional Damage to a Protected Computer
[Violation of 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B), and 2]

37. Paragraphs 1 through 31 of this indictment are re-alleged and incorporated by reference as though fully set forth herein.

38. On or about the dates listed below, in the Northern District of Texas and elsewhere, defendant **Yevgeniy Igorevich Polyanin**, 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, caused damage affecting 10 or more protected computers during a 1-year period, and caused damage affecting a computer used by and for an entity of the United States Government in furtherance of the administration of justice, described below for each count, each transmission consisting a separate count:

Count	Date	Victim
Two	August 5, 2019	Company A
Three	August 16, 2019	Company B
Four	August 16, 2019	Government Entity C
Five	August 16, 2019	Government Entity D
Six	August 16, 2019	Government Entity E
Seven	August 16, 2019	Government Entity F

Count	Date	Victim
Eight	August 16, 2019	Government Entity G
Nine	August 16, 2019	Government Entity H
Ten	August 16, 2019	Government Entity I
Eleven	August 16, 2019	Government Entity J
Twelve	August 16, 2019	Government Entity K
Thirteen	August 16, 2019	Government Entity L

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

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

39. Paragraphs 1 through 31 of this indictment are re-alleged and incorporated by reference as though fully set forth herein.

40. From on or about March 1, 2019, through on or about August 24, 2021, in the Northern District of Texas and elsewhere, defendant **Yevgeniy Igorevich Polyanin** 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)]

41. Paragraphs 1 through 40 of this indictment are realleged and incorporated by reference as though fully set forth herein.

42. Upon conviction for any offense alleged in Counts One through Thirteen of this indictment, defendant **Yevgeniy Igorevich Polyanin** 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.

43. Upon conviction for the offense alleged in Count Fourteen of this indictment, defendant **Yevgeniy Igorevich Polyanin** 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.

44. 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.

YEVGENIY IGOREVICH POLYANIN

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, 10, 11, 12, and 13)

18 U.S.C. §§ 1956(h), 1956(a)(2)(B)(i), and 1957
Conspiracy to Commit Money Laundering
(Count 14)

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

14 Counts

A true bill rendered

DALLAS FOREPERSON

Filed in open court this 24 day of August, 2021.

Warrant to be Issued

UNITED STATES MAGISTRATE JUDGE
No Criminal Matter Pending