UNITED STATES DISTRICT COURT
District of Kansas
(Kansas City Docket)

UNITED STATES OF AMERICA,

Plaintiff,

v. **CASE NO.** 24-20061-HLT-ADM

RIM JONG HYOK (림종혁),

Defendant.

INDICTMENT

THE GRAND JURY CHARGES:

INTRODUCTION

At all times relevant to this indictment:

1. North Korea's primary military intelligence agency is the Reconnaissance General Bureau (RGB). The RGB was sanctioned by the U.S. Department of Treasury in 2015, for its involvement in conventional arms trading prohibited by United Nations resolutions and malicious cyber activity. The RGB's recent cyber operations have included spreading disinformation, cyber attacks on U.S. and South Korea critical infrastructure, computer intrusions into foreign government agencies and private corporations, and revenue generation from ransom payments and cryptocurrency exchange hacks.

2. A cyber unit within the RGB is known by cybersecurity researchers as Andariel, Onyx Sleet, and Silent Chollima. The U.S. Department of the Treasury sanctioned Andariel in 2019, for its "malicious cyber operations on foreign businesses, government agencies, financial services infrastructure, private corporations, and businesses, as well as the defense industry," and because it "consistently executes cybercrime to generate revenue and targets South Korea's government and infrastructure in order to collect information and to create disorder."

3. Defendant **RIM JONG HYOK** knowingly and intentionally conspired with persons known and unknown to the grand jury (collectively, the "Conspirators") to target and access without authorization the computer networks of U.S. critical infrastructure – specifically hospitals and healthcare companies – including in the District of Kansas, using RGB-developed malware that would encrypt a victim company's computers. After successfully encrypting files, the Conspirators demanded ransoms from U.S. and South Korean hacking victims, which in turn funded the Conspirators' computer intrusions into government agencies, military bases, and companies supporting the military, including with missile, aerospace, and uranium processing technology. These hacking operations aligned with the RGB's goal of collecting information that furthers the North Korean regime's military and nuclear aspirations.

THE VICTIMS

Ransomware Victims

4. "Kansas Hospital" is a hospital located in the District of Kansas, and a May 2021 ransomware victim.

5. "Arkansas Healthcare Company" is a healthcare company providing disability services, located in the Western District of Arkansas, and a March 2022 ransomware victim.

6. "Connecticut Healthcare Company" is a healthcare company providing healthcare policy advocacy for minorities, located in the District of Connecticut, and a March 2022 ransomware victim.

7. "Florida Hospital" is a hospital located in the Middle District of Florida, and a March 2022 ransomware victim.

8. "Colorado Medical Clinic" is a medical clinic located in the District of Colorado, and a March 2022 ransomware victim.

9. "South Korean Manufacturing Company" is a manufacturing company located in the Republic of South Korea (South Korea), and a March 2023 ransomware victim.

Data Exfiltration Victims

10. The National Aeronautics and Space Administration (NASA) is a federal agency located in the District of Columbia, and a February 2022 victim.

11. "California Defense Company" is a defense contractor that designs and builds satellites, located in the Central District of California, and a March 2022 victim.

12. "Michigan Defense Company" is a defense contractor that designs and builds military equipment, located in the Eastern District of Michigan, and an April 2022 victim.

13. Randolph Air Force Base is a U.S. Air Force base, located in the Western District of Texas, and an April 2022 victim.

14. Robins Air Force Base is a U.S. Air Force base, located in the Middle District of Georgia, and an April 2022 victim.

15. "Oregon Defense Company" is a defense contractor located in the District of Oregon, and an April 2022 victim.

16. "Massachusetts Defense Company" is a defense contractor supporting U.S. military aircraft, located in the District of Massachusetts, and a November 2022 victim.

17. "Chinese Energy Company" is an energy company located in Shenzhen, People's Republic of China (PRC), and a 2022 victim.

18. "Taiwanese Defense Company" is a defense contractor headquartered in Taiwan, but with locations in the South Korea, and a 2023 victim.

19. "South Korean Defense Company 1" is a defense contractor located in South Korea, and a 2023 victim.

20. "South Korean Defense Company 2" is a defense contractor located in South Korea, and a 2023 victim.

COUNT 1
CONSPIRACY
[18 U.S.C. § 371]

21. The allegations in paragraphs 1 through 20 are re-alleged here.

22. From at least in or around May 2021, and continuing through at least in or around April 2023, in the District of Kansas and elsewhere,

RIM JONG HYOK,

the defendant, did knowingly and willfully combine, conspire, confederate, and agree with others known and unknown to the Grand Jury to commit offenses 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, including a loss aggregating at least $5,000 in value during a one-year period, damage affecting ten or more protected computers during a one-year period, and the modification or impairment of the medical examination, diagnosis, treatment, or care of one or more individuals, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B)(i);

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

(c) to intentionally access a computer without authorization and thereby obtain information from any department or agency of the United States and from any protected computer, where the value of the information obtained exceeded $5,000, in violation of 18 U.S.C. §§ 1030(a)(2)(B), 1030(a)(2)(C), and 1030(c)(2)(B).

THE OBJECT OF THE CONSPIRACY

23. The object of the conspiracy was for North Korean state-sponsored actors to hack the computers of victims, primarily U.S. hospitals and healthcare companies, to extort ransoms, and then use that money to, among other things, purchase internet servers to commit computer intrusions against U.S., South Korean, and PRC government or technology victims.

MANNER AND MEANS OF THE CRIMINAL CONSPIRACY

24. **RIM** lived in North Korea and worked in the RGB's offices in both Pyongyang and Sinuiju.

25. The RGB developed malware in furtherance of their malicious cyber operations. Some of the malware developed by the RGB and identified by private cybersecurity companies includes Valefor, VSingle, ValidAlpha, YamaBot, DTrack, TigerRAT, and MagicRAT.

26. The Conspirators used RGB-developed ransomware named Maui against U.S. hospitals and healthcare companies. Upon successful deployment, the Maui ransomware encrypted files on computers used for medical testing and electronic records and thereby disrupted healthcare services until the victim paid a ransom to the cryptocurrency address in the ransom note. If a victim made such a ransom payment, the Conspirators would provide decryption keys for the victims to access their files. This activity was the subject of a July 2022 U.S. joint Cyber Security Advisory titled "North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector."

27. The Conspirators also conducted computer intrusions for the purpose of exfiltrating sensitive information. They funded these operations, at least in part, by using the ransom money from the U.S. healthcare victims to pay for internet services, such as virtual private servers. This activity was the subject of a February 2023 international joint Cyber Security Advisory titled "Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities."

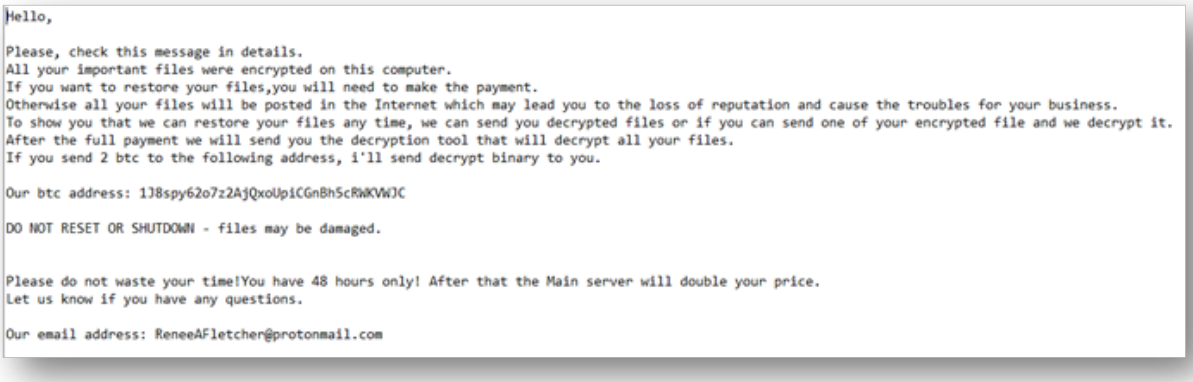
28. After the Conspirators gained initial access to the network of one of these data exfiltration victims, typically through known but unpatched vulnerabilities, they used malware to exfiltrate the victim's sensitive information to virtual private servers purchased by the Conspirators, so that the stolen information could eventually be sent to the RGB in North Korea.

OVERT ACTS

29. To further the conspiracy and advance the object of the conspiracy, the Conspirators committed the following overt acts, among others, in the District of Kansas and elsewhere:

30. On or about May 4, 2021, Conspirators gained unauthorized access to the Kansas Hospital's computer system and used a previously unseen malware tool called "Maui" – because it used a file named "maui.exe" – to encrypt four of the victim's computer servers: the intranet server, the X-ray and diagnostic imaging server, the electronic document management server, and the sleep lab server. Until the Kansas Hospital regained access to those encrypted computer servers, its medical services were limited and it had to cancel some patient appointments. The following is a screenshot of

the ransom note left on the Kansas Hospital's computer network by Conspirator 1, demanding a ransom of two Bitcoin in exchange for restoring access to the encrypted computer servers:



```
Hello,

Please, check this message in details.
All your important files were encrypted on this computer.
If you want to restore your files,you will need to make the payment.
Otherwise all your files will be posted in the Internet which may lead you to the loss of reputation and cause the troubles for your business.
To show you that we can restore your files any time, we can send you decrypted files or if you can send one of your encrypted file and we decrypt it.
After the full payment we will send you the decryption tool that will decrypt all your files.
If you send 2 btc to the following address, i'll send decrypt binary to you.

Our btc address: 1J8spy62o7z2AjQxoUpiCGnBh5cRWKVWJC

DO NOT RESET OR SHUTDOWN - files may be damaged.


Please do not waste your time!You have 48 hours only! After that the Main server will double your price.
Let us know if you have any questions.

Our email address: ReneeAFletcher@protonmail.com
```

31. On or about May 12, 2021, one day after the Kansas Hospital made a ransom payment to the cryptocurrency address specified by the hackers, Conspirator 2 transferred this Bitcoin ransom to Virtual Currency Address 1, belonging to two Hong Kong residents. This Bitcoin was converted to Tether, and then converted to Chinese yuan, before being transferred to a Chinese bank. The yuan was then accessed from an ATM in China next to the Sino-Korean Friendship Bridge connecting Dandong, China and Sinuiju, North Korea.

32. On or about June 25, 2021, Conspirator 2 transferred additional Bitcoin paid as ransom by the Kansas Hospital to Virtual Currency Address 2, which was controlled by the same two Hong Kong residents who also controlled Virtual Currency Address 1.

33. On or about March 7, 2022, Conspirators gained unauthorized access to the Arkansas Healthcare Company's computer system and deployed ransomware similar to Maui, with a file named "m.exe," to deny the Arkansas Healthcare Company access to its computer system. The Conspirators left a note on the victim's network demanding a ransom.

34. On or about March 11, 2022, Conspirators gained unauthorized access to the Connecticut Healthcare Company's computer system and deployed ransomware similar to Maui, with a file named "m.exe," to deny the Connecticut Healthcare Company access to its computer system. The Conspirators left a note on the victim's network demanding a ransom of two Bitcoin.

35. On or about March 15, 2022, Conspirators gained unauthorized access to the Florida Hospital's computer system and deployed Maui ransomware, to deny the Florida Hospital access to its computer system. The Conspirators left a note on the victim's network demanding a ransom. As part of the ransomware attack, the Conspirators used Virtual Private Server 1, which was provided by Cloud Computing Company 1 and leased by Account 1. Account 1 also leased Virtual Private Server 2 and Virtual Private Server 3 from Cloud Computing Company 1.

36. On or about March 24, 2022, Conspirators gained unauthorized access to the Colorado Medical Clinic's computer system and deployed ransomware similar to Maui, with a file named "aui.exe," to deny the Colorado Medical Clinic access to its computer system. The Conspirators left a note on the victim's network demanding a ransom of three Bitcoin. The ransomware encrypted the clinic's Electronic Health Record

system and limited the services of the clinic for a week, causing the Colorado Medical Clinic to cancel patient appointments.

37. On or about March 31, 2022, Conspirator 1 sent an email to Conspirator 2 requesting another Bitcoin address and identified Virtual Currency Address 2 – i.e., the virtual currency address to which the Kansas Hospital paid a portion of its ransom – as having been previously provided to Conspirator 1 by Conspirator 2.

38. On or about April 1, 2022, Conspirators transferred Bitcoin paid as ransom by the Colorado Medical Clinic to Virtual Currency Address 3, which was controlled by the same two Hong Kong residents who also controlled Virtual Currency Addresses 1 and 2.

39. On or about June 29, 2022, Conspirators transferred Bitcoin paid as ransom by the Colorado Medical Clinic to Cloud Computing Company 1 to make a payment for Account 1.

40. On or about July 4, 2022, **RIM** sent an email to Conspirator 1 with Virtual Currency Address 4, which was controlled by **RIM**.

41. On or about July 5, 2022, Conspirators transferred Bitcoin paid as ransom by the Connecticut Healthcare Company to Virtual Currency Address 4.

42. In or around February 2022, Conspirators used Virtual Private Server 2 and a previously unseen malware script to gain and retain unauthorized access for more than three months to NASA's computer system, specifically the portal for its Office of Inspector General, and extracted over seventeen gigabytes of unclassified data.

43. On or about March 15, 2022, Conspirators used Virtual Private Server 1 to gain and retain unauthorized access for more than a month to the California Defense Company's computer system, including by using the victim's administrator account and digital authentication certificates.

44. Beginning in or around April 2022, Conspirators used Virtual Private Server 2 and the same malware script used in the NASA hack to gain and retain unauthorized access for seven months to the Michigan Defense Company's computer network.

45. In or around April 2022, Conspirators used Virtual Private Server 2 and exploited the Log4Shell vulnerability to gain and retain unauthorized access for over two weeks to Randolph Air Force Base's computer system, before the vulnerability was remediated. The Conspirators extracted nearly a gigabyte of unclassified data. Log4Shell was a vulnerability in the widely used logging framework called Log4j.

46. In or around April 2022, Conspirators used Virtual Private Server 2 to gain and retain unauthorized access for over ten days to the Robins Air Force Base's computer system, using the Log4Shell vulnerability, before the vulnerability was remediated. The Conspirators extracted over a gigabyte of unclassified data (such as employee information and passwords) across three separate occasions.

47. Beginning in or around April 2022, Conspirators gained and retained unauthorized access for over one month to the Oregon Defense Company's computer system – using a malware script and three virtual private servers also used in the hack of NASA – and extracted over three terabytes of compressed unclassified information. The

unclassified information exfiltrated from the Oregon Defense Company included limited technical information pertaining to maritime and uranium processing projects.

48. Beginning in or around November 2022, Conspirators used Virtual Private Server 3 to gain and retain unauthorized access for several months to the Massachusetts Defense Company's computer system and extract over 30 gigabytes of data, including unclassified technical information about material used in military aircraft and satellites, much of which was from 2010 or earlier.

49. In or around 2022, Conspirators exfiltrated research and development data from the Chinese Energy Company located in Shenzhen, China. The stolen information was then stored an account that was accessed by Virtual Private Server 3.

50. On or about March 8, 2023, Conspirators falsely registered a domain name, "makingsitebeauty.com," and knowingly used it to upload and conceal exfiltrated South Korean defense technology information on Virtual Private Server 4. Virtual Private Server 4 was controlled by the same Conspirators who controlled and paid for Virtual Private Servers 1-3.

51. In or around March 2023, Conspirators gained unauthorized access to the South Korean Manufacturing Company's computer system and encrypted the company's electronic files. The Conspirators left a note on the victim's network demanding a ransom. On April 12, 2023, a payment of 4.3 Bitcoin was transferred to the Conspirators on behalf of the South Korean Manufacturing Company.

52. In or around April 2023, Conspirators moved over 250 gigabytes of stolen data (including technical and design information about military weapons and vehicles,

such as tanks, fighter jets, rockets, and torpedoes) to Virtual Private Server 4. This defense technology information included data that had been exfiltrated from the Taiwanese Defense Company, South Korean Defense Company 1, and South Korean Defense Company 2.

All in violation of Title 18, United States Code, Sections 371 and 3559(g).

COUNT 2
CONSPIRACY TO COMMIT MONEY LAUNDERING
[18 U.S.C. § 1956(h)]

53. The allegations in paragraphs 1 through 52 are re-alleged here.

54. Between in or around May 2021 and continuing through in or around April 2023, in the District of Kansas and elsewhere,

RIM JONG HYOK,

the defendant, did knowingly and willfully combine, conspire, confederate, and agree with others known and unknown to the Grand Jury to violate 18 U.S.C. § 1956(a)(1)(A)(i), that is, conducting a financial transaction affecting interstate or foreign commerce, knowing that the transaction involved the proceeds of some form of unlawful activity, with the intent to promote the specified unlawful activity, that is, unauthorized access to and obtaining information from protected computers in violation of 18 U.S.C. § 1030(a)(2)(C).

All in violation of Title 18, United States Code, Sections 1956(h) and 3559(g).

FORFEITURE NOTICE

55. The allegations contained in paragraphs 1 through 54 and Counts 1 and 2 of this Indictment are hereby realleged and incorporated by reference for the purpose of

alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(1) and 1030(i).

56. Upon conviction of the conspiracy offense set forth in Count 1, the defendant shall forfeit to the United States of America:

A. 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 such offense; and

B. pursuant to Title 18, United States Code, Section 1030(i), any personal property that was used or intended to be used to commit or to facilitate the commission of such offense.

The property to be forfeited includes, but is not limited to:

A. Money Judgment: A forfeiture money judgment imposed against the defendant in an amount equal to the proceeds obtained by the defendant as a result of such offense.

57. Upon conviction of the conspiracy offense set forth in Count 2, the defendant shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 982(a)(1), any property, real or personal, involved in such offense, or any property traceable to such property, including but not limited to, the following:

A. Money Judgment: A forfeiture money judgment imposed against the defendant in an amount equal to the value of the property involved in Count 2.

58. If any of the property described above, as a result of any act or omission of the defendant:

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 pursuant to Title 21, United States Code, Section 853(p).

All pursuant to Title 18, United States Code, Sections 982(a)(1) and 1030(i), and Title 21, United States Code, Section 853.

A TRUE BILL.

July 24, 2024
DATE

s/Foreperson
FOREPERSON OF THE GRAND JURY

KATE E. BRUBACHER
UNITED STATES ATTORNEY

By: */s/ Ryan J. Huschka*
Ryan J. Huschka
Assistant United States Attorney
Email: Ryan.Huschka@usdoj.gov
Ks. S. Ct. No. 23840

By: */s/ D. Christopher Oakley*

D. Christopher Oakley
Assistant United States Attorney
Email: Chris.Oakley@usdoj.gov
Ks. S. Ct. No. 19248

District of Kansas
500 State Avenue, Suite 360
Kansas City, Kansas 66101
Ph: (913) 551-6730
Fax: (913) 551-6541

By: */s/ Neeraj Gupta*
Neeraj Gupta
Trial Attorney
Email: Neeraj.Gupta@usdoj.gov
NY Bar No. 4770293

By: */s/ George S. Brown*
George S. Brown
Trial Attorney
Email: George.Brown3@usdoj.gov
CA Bar No. 336348

National Security Division, National Security Cyber Section
Main Justice Building
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Ph: (202) 514-2000
Fax: (202) 532-4251

IT IS REQUESTED THAT THE TRIAL BE HELD IN KANSAS CITY, KANSAS

PENALTIES

Count 1: Conspiracy

- Punishable by a term of imprisonment of not more than five years. 18 U.S.C. § 371. If the defendant knowingly falsely registered a domain name and knowingly used that domain name in the course of the offense, the maximum term of imprisonment is ten years. 18 U.S.C. § 3559(g).

- A term of supervised release of not more than three years. 18 U.S.C. § 3583(b)(2).

- A fine not to exceed $250,000. 18 U.S.C. § 3571(b)(3).

- A mandatory special assessment of $100. 18 U.S.C. § 3013(a)(2)(A).

- Forfeiture.

Count 2: Conspiracy to Commit Money Laundering

- Punishable by a term of imprisonment of not more than twenty years. 18 U.S.C. § 1956(a)(1). If the defendant knowingly falsely registered a domain name and knowingly used that domain name in the course of the offense, the maximum term of imprisonment is twenty-seven years. 18 U.S.C. § 3559(g).

- A term of supervised release of not more than three years. 18 U.S.C. § 3583(b)(2).

- A fine not to exceed $500,000 or twice the value of the property involved in the transaction, whichever is greater. 18 U.S.C. § 1956(a)(1).

- A mandatory special assessment of $100. 18 U.S.C. § 3013(a)(2)(A).

- Forfeiture.