



UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

June 2024 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

v.

RAMI KHALED AHMED,
aka "Black Kingdom,"

Defendant.

CR 2:25-cr-00335-WLH

I N D I C T M E N T

[18 U.S.C. § 371: Conspiracy; 18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I): Intentional Damage to a Protected Computer; 18 U.S.C. § 1030(a)(7)(C), (c)(3)(A): Threatening Damage to a Protected Computer]

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS AND DEFINITIONS

At all times relevant to this indictment:

1. Defendant RAMI KHALED AHMED, also known as ("aka") "Black Kingdom," ("AHMED") was a resident of Sana'a, Yemen.

2. Victim A was a construction consulting company headquartered in New Jersey.

3. Victim B was a school district in Pennsylvania.

4. Victim C was a health clinic located in Wisconsin.

1 5. Victim D was a regional steel service company headquartered
2 in Tennessee.

3 6. Victim E was a medical billing services company
4 headquartered in Encino, California, within the Central District of
5 California.

6 7. Victim F was a ski resort located in Oregon.

7 8. "Malware" is malicious computer software intended to cause
8 a victim computer to behave in a manner inconsistent with the
9 intention of the owner or user of the victim computer, usually
10 unbeknownst to that person.

11 9. "Ransomware" is a type of malware that infects a computer
12 and encrypts some or all of the data or files on the computer, and
13 then demands that the victim pay a ransom in order to decrypt and
14 recover the files, or in order to prevent the hacker from
15 distributing or destroying the data.

16 10. "Web Shell" is a computer program that enables an
17 interactive text-based interface which can be remotely accessed over
18 the internet, which is commonly used by malicious actors to gain
19 unauthorized control over a web server.

COUNT ONE

[18 U.S.C. § 371]

1. The Grand Jury re-alleges and incorporate paragraphs 1 through 10 of the Introductory Allegations of this Indictment.

A. OBJECTS OF THE CONSPIRACY

2. Beginning on a date unknown to the Grand Jury, but no later than March 18, 2021, and continuing through at least June 22, 2023, in Encino, California, within the Central District of California, and elsewhere, defendant AHMED, together with others unknown to the Grand Jury, conspired and agreed with each other to knowingly cause the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally cause damage without authorization to protected computers, and specifically:

a. to cause loss to one or more persons during a one-year period aggregating at least \$5,000 in value, in violation of Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I); and

b. to transmit in interstate and foreign commerce, with the intent to extort money and other things of value, a communication containing a demand and request for money and other things 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, Section 1030(a)(7)(C), (c)(3)(A).

B. MEANS BY WHICH THE OBJECTS OF THE CONSPIRACY WERE TO BE ACCOMPLISHED

3. The objects of the conspiracy were to be accomplished, in substance, as follows:

1 Development and Dissemination of Malware

2 a. Defendant AHMED developed the Black Kingdom malware
3 designed to acquire without authorization access to computer systems
4 through a then-existing vulnerability in Microsoft's Exchange Server
5 software. This malware was designed to primarily act as ransomware,
6 which would intentionally impair without authorization the
7 availability of the victims' data, programs, systems, and
8 information.

9 b. Defendant AHMED then conducted automated scans of
10 computer networks, both in the United States and elsewhere, to
11 identify Microsoft Exchange Servers that had not been patched to
12 address this software vulnerability and could therefore be
13 penetrated.

14 c. When defendant AHMED identified a vulnerable Microsoft
15 Exchange Server, defendant AHMED caused the transmission of malware
16 designed to place a web shell on the compromised system without the
17 knowledge or consent of the owners of the computer system.

18 Use of Malware to Conduct a Ransomware Attack

19 d. Once a web shell had been placed on a potential
20 victim's server, the Black Kingdom malware was designed to spread
21 itself across that victim's internal network of computers.

22 e. If the target computer system was connected to the
23 Internet, the Black Kingdom malware would then access a file
24 repository stored at Mega.nz and use a username and password hard-
25 coded into the Black Kingdom malware to obtain a dynamic encryption
26 key.

1 f. The Black Kingdom malware would then use this dynamic
2 encryption key to encrypt all the files on the victim's compromised
3 computer systems thus rendering them inaccessible to the victim.

4 Cyber-Enabled Extortions

5 g. If the Black Kingdom malware was successful in
6 encrypting the victim's computer system, it created a text file
7 containing a ransom note giving the victim instructions about how to
8 regain access to the victim's computer files and to prevent the data
9 from being released to the public.

10 h. The ransom note directed the victim to send \$10,000
11 worth of Bitcoin, a type of cryptocurrency, to a cryptocurrency
12 address ending in "b34FT" controlled by a coconspirator and to send
13 proof of this payment to the email address
14 support_blackkingdom2@protonmail[.]com (the Black Kingdom email).

15 i. The ransom note stated that "[a]fter you submit the
16 payment, the data will be removed from our servers, and the decoder
17 will be given to you, so that you can recover all your files."

18 j. If the Black Kingdom malware was unsuccessful in
19 encrypting the victim's computer systems, it would leave a different
20 text file ransom note telling the victim that the victim's files had
21 been uploaded to Black Kingdom's servers and would be sold on a
22 "Darknet website" if the ransom was not paid. The note also directed
23 the victim to contact the Black Kingdom email and to send \$10,000 in
24 Bitcoin to the same cryptocurrency address ending in "b34FT."

25 k. During the course of the conspiracy, the Black Kingdom
26 conspirators caused the transmission of the Black Kingdom malware to
27 approximately 1,500 computer systems in the United States and
28 elsewhere.

1 C. OVERT ACTS

2 4. In furtherance of the conspiracy, and to accomplish its
3 objects, defendant AHMED, together with others unknown to the Grand
4 Jury, on or about the dates set forth below, committed and caused to
5 be committed various overt acts, in the Central District of
6 California and elsewhere, including, but not limited to, the
7 following:

8 Overt Act No. 1: On an unknown date, but no later than March
9 18, 2021, defendant AHMED created the Black Kingdom malware which was
10 designed to intentionally impair without authorization the
11 availability of computer systems through a then-existing
12 vulnerability in Microsoft's Exchange software.

13 New Jersey

14 Overt Act No. 2: On an unknown date, but no later than March
15 18, 2021, defendant AHMED knowingly caused the transmission of the
16 Black Kingdom malware to a computer system belonging to Victim A.

17 Overt Act No. 3: On March 18, 2021, defendant AHMED, through
18 the Black Kingdom malware, encrypted data belonging to Victim A
19 rendering them inaccessible.

20 Overt Act No. 4: On March 18, 2021, after the conspirators
21 received \$10,000 in Bitcoin from Victim A, defendant AHMED emailed a
22 representative of Victim A to provide a purported decryption key.

23 Pennsylvania

24 Overt Act No. 5: On an unknown date, but no later than March
25 18, 2021, defendant AHMED knowingly caused the transmission of the
26 Black Kingdom malware to a computer system belonging to Victim B.

1 Overt Act No. 6: On March 18, 2021, defendant AHMED, through
2 the Black Kingdom malware, encrypted data belonging to victim B
3 rendering them inaccessible.

4 Wisconsin

5 Overt Act No. 7: On an unknown date, but no later than March
6 18, 2021, defendant AHMED knowingly caused the transmission of the
7 Black Kingdom malware to a computer system belonging to Victim C.

8 Overt Act No. 8: On March 18, 2021, defendant AHMED, through
9 the Black Kingdom malware, encrypted data belonging to Victim C
10 rendering them inaccessible.

11 Tennessee

12 Overt Act No. 9: On an unknown date, but no later than March
13 20, 2021, defendant AHMED knowingly caused the transmission of the
14 Black Kingdom malware to a computer system belonging to Victim D.

15 Overt Act No. 10: On March 20, 2021, defendant AHMED, through
16 the Black Kingdom malware, encrypted data belonging to Victim D
17 rendering them inaccessible.

18 California

19 Overt Act No. 11: On an unknown date, but no later than March
20 21, 2021, defendant AHMED knowingly caused the transmission of the
21 Black Kingdom malware to a computer system belonging to Victim E.

22 Overt Act No. 12: On or about March 18, 2021, defendant
23 AHMED, through the Black Kingdom Malware, encrypted data belonging to
24 Victim E rendering them inaccessible.

25 Oregon

26 Overt Act No. 13: On an unknown date, but no later than June
27 21, 2023, defendant AHMED knowingly caused the transmission of the
28 Black Kingdom malware to a computer system belonging to Victim F.

COUNT TWO

[18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I)]

On or about March 20, 2021, in Los Angeles County, within the Central District of California, and elsewhere, defendant RAMI KHALED AHMED, also known as ("aka") "Black Kingdom," ("AHMED"), knowingly caused the transmission of a program, information, code and command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, as that term is defined in Title 18, United States Code, Section 1030(e)(2)(B), owned by Victim E, thereby causing loss to one or more persons during a one-year period aggregating at least \$5,000 in value.

COUNT THREE

[18 U.S.C. §§ 1030(a)(7)(C), (c)(3)(A)]

On or about March 20, 2021, in Los Angeles County, within the Central District of California, and elsewhere, defendant RAMI KHALED AHMED, also known as ("aka") "Black Kingdom," ("AHMED"), with intent to extort from Victim E money and other things of value, transmitted in interstate and foreign commerce, a communication containing a demand and request for money and other things of value in relation to damage to a protected computer, as that term is defined in Title 18, United States Code, Section 1030(e)(2)(B), belonging to Victim E, where such damage was caused to facilitate the extortion.

A TRUE BILL

/s/
Foreperson

BILAL A. ESSAYLI
United States Attorney



DAVID T. RYAN
Assistant United States Attorney
Chief, National Security Division

KHALDOUN SHOBAKI
Assistant United States Attorney
Chief, Cyber and Intellectual
Property Crimes Section

ALEXANDER S. GORIN
ANGELA C. MAKABALI
Assistant United States Attorneys
Cyber and Intellectual Property
Crimes Section