

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

-v.-

HOSSEIN HAROONI,
REZA KAZEMIFAR,
KOMEIL BARADARAN SALMANI, and
ALIREZA SHAFIE NASAB,

Defendants.

SEALED
SUPERSEDING
INDICTMENT

S1 21 Cr. 704

COUNT ONE

(Conspiracy to Commit Computer Intrusions)

The Grand Jury charges:

OVERVIEW

1. From at least in or about 2016 through at least in or about April 2021, HOSSEIN HAROONI (حسین هارونی), REZA KAZEMIFAR (رضا کاظمی فر), KOMEIL BARADARAN SALMANI (کمیل برادران سلمانی), and ALIREZA SHAFIE NASAB (علیرضا شفیعی نسب), the defendants, nationals of the Islamic Republic of Iran, and others known and unknown, were members of a hacking organization that participated in a coordinated, multi-year campaign to conduct and attempt computer intrusions into more than a dozen American companies and the U.S. Departments of the Treasury and State.

2. The private sector victims were primarily cleared defense contractors, which were granted security clearances by the U.S. Department of Defense to access, receive, and store classified information for the purpose of conducting activities in support of U.S. Defense

Department programs. Other private sector victims included a New York, New York-based accounting firm, where more than 200,000 employee accounts were compromised, and a New York, New York-based hospitality company (“Hospitality Company-1”), where more than 2,000 employee accounts were targeted for compromise.

MEANS AND METHODS OF THE CONSPIRACY

Spearphishing

3. In conducting their hacking campaign, one of the means through which members of the conspiracy obtained and sought to obtain unauthorized access to victim systems was through the use of spearphishing. In a spearphishing campaign, a malicious actor sends an email or other online message to a victim, which message attempts to trick the victim into either clicking a link that will download malicious software (“malware”) onto the victim’s computer or unwittingly providing account credentials (*i.e.*, username and password) to the malicious actor.

4. Members of the conspiracy created, and used, a particular application they named “Dandelion” to manage their many spearphishing campaigns. The Dandelion application enabled members of the conspiracy to obtain a report of various target email accounts for different campaigns (including whether a particular target email account clicked the malicious hyperlink in spearphishing emails as well as the victim Internet protocol (“IP”) address, victim location, the web browser used by the victim, and the victim’s operating system). “Dandelion” also allowed conspiracy members to select which email accounts to target and then launch spearphishing attacks.

5. In many instances, members of the conspiracy registered domains that were designed to mimic the domains of victim entities or other known corporate entities, to trick recipients into believing that the spearphishing emails came from a trusted source. In other

instances, members of the conspiracy leveraged compromised accounts, or fraudulently created accounts on victim systems, to use those accounts, and the associated authentic and trusted domains, to target additional victims.

6. For example, between in or about February 2019 and in or about December 2019, members of the conspiracy targeted two cleared defense contractors ("Defense Contractor-1" and "Defense Contractor-2") and a consulting firm ("Consulting Firm-1"). In or about August 2019, the conspirators compromised an administrator email account belonging to Defense Contractor-1. After obtaining unauthorized access to that account, the conspirators used the account's administrator privileges to create two new unauthorized Defense Contractor-1 email accounts. The conspirators then used those two fraudulent email accounts to send spearphishing emails to employees of Defense Contractor-2 and Consulting Firm-1, in the course of attempting to compromise the computer systems of Defense Contractor-2 and Consulting Firm-1.

Social Engineering

7. Members of the conspiracy also used social engineering, which is the use of deception to manipulate individuals into divulging confidential or personal information, in order to gain unauthorized access to victim accounts and networks. Generally, the conspirators sent messages to victims from conspirator-created social media accounts with female personas. These messages often contained links to a malicious domain or attached documents embedded with malware.

8. For example, the conspirators used social engineering involving a female persona to induce an employee at Defense Contractor-2 to click on a link in a web form. Shortly thereafter, members of the conspiracy compromised that employee's account at Defense Contractor-2.

THE DEFENDANTS

9. At all times relevant to this Superseding Indictment ("Indictment"), HOSSEIN HAROONI, REZA KAZEMIFAR, KOMEIL BARADARAN SALMANI, and ALIREZA SHAFIE NASAB, the defendants, participated in the above-described highly organized and coordinated scheme to conduct computer intrusions targeting American companies and federal agencies. During their involvement in the crimes charged in this Indictment, HAROONI, KAZEMIFAR, SALMANI, and NASAB worked for Iran-based private technology companies, and had the following roles in the conspiracy:

a. HAROONI was responsible for procuring, administering, and managing the online network infrastructure, including but not limited to computer servers and customized software used to facilitate the computer intrusions. HAROONI also fraudulently used the identity of a real person ("Individual-1"), including his use of a copy of Individual-1's true passport, in order to conceal his role in procuring online infrastructure used by the conspiracy to facilitate the computer intrusion campaign.

b. KAZEMIFAR was responsible for testing the tools utilized by the conspiracy to execute its cyber campaigns. For example, KAZEMIFAR was involved in testing spearphishing emails used to target, among other entities, Hospitality Company-1. KAZEMIFAR was also involved in developing malware utilized by the conspiracy in social engineering initiatives. During the course of his involvement in the conspiracy, from at least in or about 2014 through at least in or about 2020, KAZEMIFAR also worked for the Iranian Organization for Electronic Warfare and Cyber Defense ("EWCD"). EWCD is a component of the Islamic Revolutionary Guard Corps ("IRGC"), which is itself a component of the Iranian Armed Forces.

Among other things, the IRGC is responsible for Iran's offensive cyber capabilities. The United States has designated IRGC as a foreign terrorist organization.

c. BARADARAN SALMANI was responsible for testing tools utilized by the conspiracy to execute spearphishing campaigns, including the campaign against Hospitality Company-1. SALMANI was also involved in maintaining infrastructure used by the conspirators.

d. SHAFIE NASAB was responsible for procuring infrastructure used by the conspiracy, particularly infrastructure used in furtherance of social engineering campaigns. NASAB also used Individual-1's identity, including Individual-1's name and passport, to register server and email accounts that were used during cyber campaigns.

e. At all times relevant to this Superseding Indictment, Mahak Rayan Afraz (منحک رایان افراز) ("MRA") was an Iran-based company that purported to provide cybersecurity services. KAZEMIFAR, BARADARAN SALMANI, and SHAFIE NASAB worked at MRA, including at times during which they engaged in the conspiracy described in this Superseding Indictment.

STATUTORY ALLEGATIONS

10. From at least in or about 2016 through at least in or about April 2021, in the Southern District of New York and elsewhere, HOSSEIN HAROONI, REZA KAZEMIFAR, KOMEIL BARADARAN SALMANI, and ALIREZA SHAFIE NASAB, the defendants, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit offenses against the United States, to wit, a computer intrusion and intentionally causing damage to a computer system, in violation of Title

18, United States Code, Sections 1030(a)(4), 1030(c)(3)(A), 1030(a)(5)(A), 1030(c)(4)(A)(i)(I), and 1030(c)(4)(B)(i) and (ii).

11. It was a part and an object of the conspiracy that HOSSEIN HAROONI, REZA KAZEMIFAR, KOMEIL BARADARAN SALMANI, and ALIREZA SHAFIE NASAB, the defendants, and others known and unknown, knowingly and with the intent to defraud, would and did access a protected computer without authorization, and exceed authorized access, and by means of such conduct further the intended fraud and obtain anything of value, in violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A).

12. It was further a part and an object of the conspiracy that HOSSEIN HAROONI, REZA KAZEMIFAR, KOMEIL BARADARAN SALMANI, and ALIREZA SHAFIE NASAB, the defendants, and others known and unknown, knowingly would and did cause the transmission of a program, information, code, and command, and as a result of such conduct, would and did intentionally cause damage, without authorization, to a protected computer, which caused a loss (including loss resulting from a related course of conduct affecting one and more other protected computers) aggregating to at least \$5,000 in value to one and more persons during any one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(A)(i)(I), and 1030(c)(4)(B)(i).

Overt Acts

13. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. In or about December 2018, members of the conspiracy sent spearphishing emails and two documents embedded with malware to an email account of Hospitality Company-1 located in New York, New York.

b. In or about September 2019, members of the conspiracy compromised an administrator account at Defense Contractor-1, used that account to create two new unauthorized email accounts on Defense Contractor-1's system, and then used those fraudulent email accounts to send spearphishing emails to additional victims.

c. In or about September 2019, HOSSEIN HAROONI, the defendant, leased a server in furtherance of the computer intrusions against Defense Contractors-1 and -2 and Consulting Firm-1.

d. In or about October 2019, HAROONI leased a server to host a malicious domain, which hosted malware used to compromise victim computer systems.

e. In or about October 2018, REZA KAZEMIFAR, the defendant, received test emails in preparation for spearphishing campaigns.

f. In or about February 2018, and in or about September 2019, KOMEIL BARADARAN SALMANI, the defendant, received test emails in preparation for spearphishing campaigns.

g. In or about September 2020, ALIREZA SHAFIE NASAB, the defendant, registered an account with an internet-service provider that leased IP addresses used as part of social engineering attacks against employees at a domestic cleared defense contractor.

(Title 18, United States Code, Section 371.)

COUNT TWO
(Conspiracy to Commit Wire Fraud)

The Grand Jury further charges:

14. The allegations contained in paragraphs 1 through 9 of this Indictment are repeated and realleged as if fully set forth herein.

15. From at least in or about 2016 through at least in or about April 2021, in the Southern District of New York and elsewhere, HOSSEIN HAROONI, REZA KAZEMIFAR, KOMEIL BARADARAN SALMANI, and ALIREZA SHAFIE NASAB, the defendants, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

16. It was a part and object of the conspiracy that HOSSEIN HAROONI, REZA KAZEMIFAR, KOMEIL BARADARAN SALMANI, and ALIREZA SHAFIE NASAB, the defendants, and others known and unknown, knowingly having devised and intending to devise a scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343, to wit, HAROONI, KAZEMIFAR, SALMANI, NASAB and others engaged in a scheme to use fraudulent means, including spearphishing, to obtain dominion and control over victim email accounts, and to create fraudulent email accounts on victim computer systems, with the intention of using those fraudulent email accounts to compromise other online accounts belonging to the same victim and other

victims, which involved the use of interstate wires into and out of the Southern District of New York.

(Title 18, United States Code, Section 1349.)

COUNT THREE
(Knowingly Damaging a Protected Computer)

The Grand Jury further charges:

17. The allegations contained in paragraphs 1 through 9 of this Indictment are repeated and realleged as if fully set forth herein.

18. From at least in or about August 2019 through at least in or about September 2019, in the Southern District of New York and elsewhere, HOSSEIN HAROONI, the defendant, who will first be brought to the Southern District of New York, 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, which caused a loss (including loss resulting from a related course of conduct affecting one and more other protected computers) aggregating to at least \$5,000 in value to one and more persons during any one-year period, to wit, HAROONI conducted, and aided and abetted, the computer intrusion of a Defense Contractor-1 administrator account and leveraged that account to create, without authorization, two fraudulent Defense Contractor-1 email accounts, which impaired the integrity of Defense Contractor-1's systems and cause a loss exceeding \$5,000.

(Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(A)(i)(I),
1030(c)(4)(B)(i), and 2; Title 18, United States Code, Section 3238.)

COUNT FOUR
(Wire Fraud)

The Grand Jury further charges:

19. The allegations contained in paragraphs 1 through 9 of this Indictment are repeated and realleged as if fully set forth herein.

20. From at least in or about May 2014 through at least in or about April 2017, in the Southern District of New York and elsewhere, HOSSEIN HAROONI, REZA KAZEMIFAR, KOMEIL BARADARAN SALMANI, and ALIREZA SHAFIE NASAB, the defendants, who will first be brought to the Southern District of New York, knowingly having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, to wit, HAROONI, KAZEMIFAR, SALMANI, NASAB and others engaged in a scheme to use fraudulent means, including spearphishing, to obtain dominion and control over victim email accounts, and to create fraudulent email accounts on victim computer systems, with the intention of using those fraudulent email accounts to compromise other online accounts belonging to the same victim and other victims, which involved the use of interstate wires into and out of the Southern District of New York.

(Title 18, United States Code, Sections 1343 and 2;
Title 18, United States Code, Section 3238).

COUNT FIVE
(Aggravated Identity Theft)

The Grand Jury further charges:

21. The allegations contained in paragraphs 1 through 9 of this Indictment are repeated and realleged as if fully set forth herein.

22. From at least in or about August 2019 through at least in or about April 2021, in the Southern District of New York and elsewhere, HOSSEIN HAROONI, the defendant, knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), and aided and abetted the same, to wit, HAROONI transferred, possessed, and used, and aided and abetted the transfer, possession, and use of, the name and passport of Individual-1 to procure computer servers during and in relation to the computer fraud and wire fraud offenses charged in Counts Two through Four of this Indictment.

(Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), and 2.)

COUNT SIX
(Aggravated Identity Theft)

The Grand Jury further charges:

23. The allegations contained in paragraphs 1 through 9 of this Indictment are repeated and realleged as if fully set forth herein.

24. From at least in or about 2017 through at least in or about 2019, in the Southern District of New York and elsewhere, ALIREZA SHAFIE NASAB, the defendant, knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), and aided and abetted the same, to wit, NASAB transferred, possessed, and used, and aided and abetted the transfer, possession, and use of, the name and passport of Individual-2 to register server and email accounts that were used for operational purposes during and in relation to the computer fraud and wire fraud offenses charged in Counts Two and Four of this Indictment.

(Title 18, United States Code, Sections 1028A(a)(1),
1028A(b), and 2.)

FORFEITURE ALLEGATIONS

25. As a result of committing the computer fraud offenses alleged in Counts One and Three of this Indictment, HOSSEIN HAROONI, REZA KAZEMIFAR, KOMEIL BARADARAN SALMANI, and ALIREZA SHAFIE NASAB, the defendants, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 1030(i), any and all property, real or personal, constituting or derived from, any proceeds obtained directly or indirectly, as a result of said offenses, and any and all personal property that was used or intended to be used to commit or to facilitate the commission of said offenses, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offenses.

26. As a result of committing the wire fraud offenses alleged in Counts Two and Four of this Indictment, HOSSEIN HAROONI, REZA KAZEMIFAR, KOMEIL BARADARAN SALMANI, and ALIREZA SHAFIE NASAB, the defendants, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), any and all property, real and personal, which constitutes or is derived from proceeds traceable to the commission said offenses, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offenses.

Substitute Assets Provision

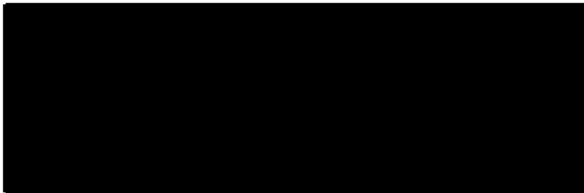
27. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:


- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third person;

- 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 subdivided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), and Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of the defendants up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 981 & 1030;
Title 21, United States Code, Section 853; and
Title 28, United States Code, Section 2461.)





DAMIAN WILLIAMS
United States Attorney