IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	**UNDER SEAL**
	)	
v.	)	Criminal No. 1:20-CR-217
	)	
SAID POURKARIM ARABI, (Counts 1 through 9)	)	Count 1: Conspiracy to Commit Computer Intrusions (18 U.S.C. § 371)
MOHAMMAD REZA ESPARGHAM, (Counts 1 through 6 and Count 9)	)	Count 2: Obtaining Information by Unauthorized Access to Protected Computers (18 U.S.C. § 1030(a)(2)(C))
and	)	
MOHAMMAD BAYATI, (Counts 1 and 9)	)	Count 3-6: Intentional Damage to Protected Computers (18 U.S.C. § 1030(a)(5)(A))
Defendants.	)	Counts 7-8: Aggravated Identity Theft (18 U.S.C. § 1028A)
	)	Count 9: Conspiracy to Commit Wire Fraud (18 U.S.C. § 1349)
	)	Forfeiture Notice: 18 U.S.C. §§ 1030(i); 981(a)(1)(C); 28 U.S.C. § 2461(c)

INDICTMENT

September 2020 Term – at Alexandria

COUNT ONE
(Conspiracy to Commit Unauthorized Computer Intrusions)

THE GRAND JURY CHARGES THAT:

1. At all times relevant to this Indictment, SAID POURKARIM ARABI, MOHAMMAD REZA ESPARGHAM, and MOHAMMAD BAYATI, the defendants, were nationals of the Islamic Republic of Iran ("Iran") living and working within Iran. ARABI was a member of the Islamic Revolutionary Guard Corps ("IRGC"), an Iranian military and intelligence organization with the primary mission of protecting the country's political system. ESPARGHAM and BAYATI were associates of IRGC member ARABI.

2. Between approximately July 2015 and February 2019, the defendants possessed a target list of over 1,800 online accounts, including accounts belonging to organizations and companies involved in aerospace or satellite technology and international government organizations in the United States, the United Kingdom, Singapore, Australia, and Israel, and sent spear phishing emails to many of those accounts. In connection with the spear phishing, the defendants engaged in a coordinated campaign of social engineering that resulted in the theft of United States citizens' identities, which the defendants used to steal and attempt to steal critical information related to U.S. aerospace and satellite technology and resources, including sensitive commercial information, intellectual property, and personal data. The defendants conducted this activity at the direction of the IRGC, whose directives were passed through defendant SAID POURKARIM ARABI.

BACKGROUND ON THE DEFENDANTS AND RELATED ENTITIES

3. The Government of Iran is a foreign power with which the United States has no formal diplomatic relations. The U.S. Secretary of State has designated Iran a state sponsor of terrorism each year since 1984; Iran is one of only four foreign countries so designated.

4. The IRGC plays an important role in bolstering Iran's economy, including its telecommunications and aerospace industries. As of 2019, the United States has designated the IRGC as a foreign terrorist organization as a result of the IRGC's participation, financing, and promotion of terrorism as a tool of statecraft.

5. At all times relevant to this Indictment, Defendant SAID POURKARIM ARABI ("ARABI") was a member of the IRGC, living in IRGC housing, working in intelligence regarding IRGC air, space, and cyber operations. As of August 15, 2015, ARABI's résumé listed his occupation as an intelligence officer and operations manager for IRGC air, space, and cyber. His résumé also touted hacking projects that he claimed to have completed, including the unauthorized access to servers at: (1) a company in partnership with an American multinational corporation invested in aerospace and satellites; and (2) an aviation company in the United Kingdom.

6. At all times relevant to this Indictment, Defendant MOHAMMAD REZA ESPARGHAM ("ESPARGHAM"), a/k/a "Reza Darkcoder" and "M.R.S.CO," was an Iranian national, living and working in Iran. ESPARGHAM was a leader of the Iranian Dark Coders Team, a notorious group of Iranian hackers responsible for numerous computer intrusions worldwide. ESPARGHAM was also the creator of VBscan, a tool utilized to detect vulnerabilities in a proprietary internet forum software package known as Vbulletin. As of September 2, 2015, ESPARGHAM's résumé listed his alias as "M.R.S.CO" and noted his

technical programming and computer infiltration skills. ESPARGHAM explained his capabilities as a website penetration or "pentest" expert, security tools programmer, and researcher of network security and vulnerability detection.

7. At all times relevant to this Indictment, Defendant MOHAMMAD BAYATI ("BAYATI") was an Iranian national living and working in Iran. BAYATI provided malicious computer code (also known as malware) for ARABI and ESPARGHAM to use in compromising victim computers.

INDIVIDUAL VICTIMS

8. VICTIM PERSON 1 is a United States resident. A member of the Conspiracy used VICTIM PERSON 1's identity to register domains used in scheme and impersonated VICTIM PERSON 1.

9. VICTIM PERSON 2 is a United States resident working as a professor at an identified public university ("UNIVERSITY 1"). A member of the Conspiracy used VICTIM PERSON 2's identity and position at UNIVERSITY 1, without his knowledge or consent, to entice individuals receiving emails falsely appearing to be from VICTIM PERSON 2 to click on malicious links in the emails. As detailed herein, clicking on the malicious links would result in the installation of malware on victims' protected computers, thereby enabling the Conspirators to gain and maintain unauthorized access to the protected computers.

VICTIM COMPANIES

10. VICTIM COMPANY 1 was a company that provided real-time satellite tracking.

11. VICTIM COMPANY 2 was a company that provided satellite voice and data communication services to its customers.

DEFINITIONS

12. The following definitions explain the terms used in this Indictment:

a. "Backdoor" is a method, often hidden, of bypassing normal authentication or encryption protocols in a computer system.

b. "Computer" is defined in Title 18, United States Code, Section 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

c. "Domain" is short for "domain name." Under Title 18, United States Code, Section 3559(g)(2)(B), the definition of "domain name" is based on the Trademark Act, Title 15, United States Code, Section 1127. Under the Trademark Act, "domain name" means "any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet."

d. "Hosting" is a service through which storage and computing resources are provided to a customer. An entity providing such services is often called a "host."

e. "IP Address" is short for "Internet Protocol Address," which is a numerical label assigned to each device connected to a computer network. Generally, an IP address serves two main functions: (1) computer or network interface identification, and (2) location addressing.

f. "Malware" is malicious software. Once a computer system is compromised with malware, a malicious actor can often install various tools, which can provide the actor with persistent access to compromised networks and computers.

g. "Metasploit Framework" is a penetration-testing platform that allows the writing, testing, and execution of computer code. The framework contains a suite of tools that users can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection.

h. "Mimikatz" is an open-source application that allows users to view and save authentication credentials. Mimikatz are commonly used by malicious actors to steal credentials or to escalate privileges on a computer network without authorization.

i. "NanoCore" is a Remote Access Trojan often spread by means of spear phishing attacks.

j. "Protected Computer" is defined in Title 18, United States Code, Section 1030(e)(2) and means a computer which is used in or affecting interstate or foreign commerce or communication. Servers that are used in or that affect interstate commerce qualify as protected computers.

k. "Python Backdoor" is an open source backdoor made in the Python programming language.

l. "Remote Access Trojan" is commonly known as a "RAT," and is a type of malware that controls a system through a remote network connection.

m. "Remote Network Connection" is a connection to a network that allows users to access the network remotely.

n. "Rial" is the official currency of Iran.

o. A "server" is a type of computer or device on a network that manages network resources.

p. "Spear phishing" is a type of email or other electronic communications scam targeting a specific individual, organization, or business.

q. "TLE" is an acronym for "Two Line Element set," which is a data format encoding a list of orbital elements of an Earth-orbiting object for a given point in time.

r. "vBulletin" was a proprietary Internet forum software package.

OBJECTS OF THE CONSPIRACY

13. From at least in or about July 2015 through at least in or about February 2019, in the Eastern District of Virginia and elsewhere, defendants ARABI, ESPARGHAM, and BAYATI, and others known and unknown to the Grand Jury, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit computer intrusion offenses in violation of Title 18, United States Code, Section 1030(a)(2)(C), 1030(a)(5)(A), 1030(c)(2)(B)(ii) and (iii), and 1030(c)(4)(B)(i).

14. It was part and an object of the Conspiracy that defendants ARABI, ESPARGHAM, and BAYATI, and others known and unknown, would and did intentionally access computers without authorization, and thereby would and did obtain information from protected computers in furtherance of a violation of the Constitution or laws of the United States or of any State (including Title 18, United States Code, Section 1343) and the value of the

information obtained would and did exceed $5,000, in violation of Title 18, United States Code, Section 1030(a)(2)(C), 1030(c)(2)(B)(ii) and (iii).

15. It was further part and an object of the Conspiracy that defendants ARABI, ESPARGHAM, and BAYATI, and others known and unknown, did knowingly cause the transmission of a program, information, code, and command and, as a result of such transmission, intentionally and without authorization caused damage to protected computers in violation of Title 18, United States Code, Section 1030(a)(5)(A) and 1030(c)(4)(B)(i).

MANNER AND MEANS OF THE CONSPIRACY

16. The Conspirators obscured their real identities and connections to Iran and the IRGC by using false identities, registering fraudulent email accounts, creating fraudulent social media accounts (including LinkedIn accounts in the names of victims' employees), and other forms of deception. To avoid detection, the Conspirators used victim computers or other domains, including domains hosted in the United States, as "hop points" to conceal their true IP addresses and locations.

17. The Conspiracy proceeded in several steps. First, the Conspirators identified individuals connected to the U.S. aerospace and satellite industry, including individuals located within the Eastern District of Virginia, whose identities the Conspirators could assume in furtherance of the scheme. The Conspirators then impersonated those individuals and used their stolen identities to register email addresses and fraudulently purchase domains and hacking tools.

18. Second, a member of the Conspiracy created customized spear phishing emails that purported to be from the individuals whose identities the Conspirators had stolen. The spear phishing emails were designed to entice unsuspecting recipients into taking a particular action—usually clicking on a malicious link. A member of the Conspiracy sent these spear phishing

emails to myriad accounts, including accounts used by the employees of U.S. aerospace and satellite technology companies.

19. Third, once a recipient clicked on a malicious link, the recipient's protected computer would connect to an online resource that hosted malware, typically "Remote Access Trojan" malware. The recipient's protected computer would then automatically download the malware, which gave the Conspirators unauthorized access to the recipient's protected computer and network. Using this method, the Conspirators successfully hacked multiple victim networks, including servers located within the Eastern District of Virginia.

20. Fourth, once a member of the Conspiracy gained access to a victim's network, the Conspirators used various exploits to create additional backdoors into the network. A member of the Conspiracy also deployed additional malware that allowed the Conspirators to gain access credentials, escalate their privileges, and maintain their unauthorized access to victim networks.

21. Finally, the Conspirators extracted data from the victim networks.

DEFENDANTS' ROLES IN THE CONSPIRACY

SAID POURKARIM ARABI

22. Defendant SAID POURKARIM ARABI used numerous email accounts to disguise his involvement in the Conspirators' spear phishing and hacking operation. For example, ARABI and other Conspirators used tleanalyser@gmail.com, lose.angles@gmail.com, reseller.apples@gmail.com, and [Business A]@gmail.com to send spear phishing emails, to purchase domains they knew would be used in furtherance of the scheme, and to facilitate information sharing among the Conspirators to further the scheme.

23. In furtherance of the scheme, Defendant ARABI procured multiple domains and virtual private servers to which IP addresses were assigned. For example, ARABI was the

registrant for mail-db.com, a domain hosted in Iran and used by the Conspirators. In addition, in May 2016 and April 2017, ARABI obtained IP addresses that were used in a 2017 computer intrusion at VICTIM COMPANY 2.

24. Between September 17, 2016 and December 11, 2018, the Conspirators conducted online reconnaissance of VICTIM COMPANY 2 and used email account reseller.apples@gmail.com to send spear phishing emails purporting to be from VICTIM PERSON 1 or VICTIM PERSON 2.

25. From on or about September 17, 2016 through September 29, 2016, the email account reseller.apples@gmail.com was used by the Conspirators to send links to malicious code hosted at a Dropbox account to spear phishing victims. As described herein, a member of the Conspiracy fraudulently registered the Dropbox account in the name of VICTIM PERSON 2.

26. From on or about May 26, 2017 through on or about October 9, 2017, ARABI registered other online communications and payment accounts in the name of VICTIM PERSON 1.

MOHAMMAD REZA ESPARGHAM

27. Among other roles, defendant MOHAMMAD REZA ESPARGHAM identified targets for the Conspirators' spear phishing and hacking operation. On July 5, 2015, for example, ESPARGHAM provided ARABI a list of over 1,800 email accounts for targeting in the spear phishing campaign. The list included spear phishing victims in the Eastern District of Virginia, such as employees of VICTIM COMPANY 2.

MOHAMMAD BAYATI

28. Defendant MOHAMMAD BAYATI provided ARABI malware to use in the scheme. Specifically, on September 3, 2016, BAYATI provided ARABI with a link to a

Dropbox account containing malicious code. ARABI responded he would "test" it later that day. The malware provided by BAYATI was associated with an IP address. The spreadsheet containing the target list referenced in paragraph 27 also contained a separate tab listing numerous IP addresses. The IP address associated with the malware sent to ARABI by BAYATI was on that list. Additionally, the type of malware that BAYATI provided ARABI was a NanoCore RAT, which is a type of malware used to compromise the networks of VICTIM COMPANY 2.

OVERT ACTS IN FURTHERANCE OF THE CONSPIRACY

29. A member of the Conspiracy obtained a PayPal account on October 30, 2011, which the Conspirators subsequently used to purchase tools and domains for use in the scheme.

30. On or about July 5, 2015, ESPARGHAM sent a file to lose.angles@gmail.com, an account controlled by ARABI. The file contained a target list of over 1,800 accounts, including accounts that received spear phishing emails sent by the Conspirators.

31. On May 19, 2016, ARABI obtained configuration and login information for the server assigned IP address 91.210.107.120, which was an IP address used in the subsequent 2017 computer intrusion at VICTIM COMPANY 2. Likewise, on April 19, 2017, ARABI obtained configuration and login information for the server assigned IP address 109.236.81.86—another IP address used in the subsequent 2017 computer intrusion at VICTIM COMPANY 2.

32. In or about July 2017, VICTIM PERSON 1's name and physical address were added to the existing PayPal account.

33. The Conspirators subsequently used the PayPal account to make a membership payment to an online search engine that allows users to find specific types of computers connected to the internet using a variety of filters. This service, which can be used lawfully by

companies seeking to identify vulnerabilities in their own systems, would have allowed the Conspirators to identify servers to target for hacking, and to discover potential points of unlawful access to those servers.

34. On multiple occasions, a member of the Conspiracy accessed the PayPal account from hacking infrastructure that the Conspirators used to gain unauthorized access to VICTIM COMPANY 2's Microsoft Office 365 account, via, among other methods, the impersonation of a VICTIM COMPANY 2 administrator.

35. Other instances of the Conspirators using the identity of VICTIM PERSON 1 to purchase fraudulent domain names and virtual private servers include:

a. On or about May 31, 2016, a member of the Conspiracy registered a fraudulent domain, [Business A].com, in the name of VICTIM PERSON 1, an employee of Business A. An invoice for this registration was sent to the Conspirators at [Business A]@gmail.com, an account controlled by ARABI.

b. On or about May 26, 2017, a member of the Conspiracy registered another fraudulent domain, tleanalyser.com, in the name of VICTIM PERSON 1. The registration listed the physical address of VICTIM COMPANY 1. An invoice for this registration, which indicated that tleanalyser.com had been purchased for 312,100 Iranian Rial, was likewise sent to the Conspirators at [Business A]@gmail.com. As detailed below, the Conspirators subsequently used tleanalyser.com to distribute malware in furtherance of the scheme.

c. Between June 14, 2017 and June 16, 2017, a member of the Conspiracy sent approximately 15 test spear phishing emails from info@tleanalyser.com to

ARABI's tleanalyser@gmail.com. The spear phishing emails were signed as having originated from VICTIM COMPANY 1.

36. In furtherance of the scheme, the Conspirators also used the identity of VICTIM PERSON 2, a professor at UNIVERSITY 1 who had numerous contacts within the satellite and aerospace industries. A member of the Conspiracy used an email account to impersonate VICTIM PERSON 2 and send spear phishing emails that appeared to be from VICTIM PERSON 2's university email address, but which actually contained malicious links to malware hosted on domains controlled by the Conspirators. The Conspirators thus used VICTIM PERSON 2's identity to entice individuals to click on the malicious links.

37. On or about September 3, 2016, BAYATI provided ARABI a link to a Dropbox account containing malware that needed to be tested in order to be used in furtherance of the scheme. ARABI indicated he would "test" it later that day. The malware was a NanoCore RAT, one of the types of malware used to compromise VICTIM COMPANY 2's networks.

38. Between September 17, 2016 and December 11, 2018, a member of the Conspiracy used email account reseller.apples@gmail.com to send spear phishing emails purporting to be from VICTIM PERSON 1 or VICTIM PERSON 2.

39. For example, on or about September 17, 2016, a member of the Conspiracy sent the following email purporting to be from VICTIM PERSON 2:

From: [redacted]@[redacted]
Sent: Saturday, September 17, 2016 10:35 AM
To: [redacted]@[redacted]
Subject: [redacted] parallel image processing project

Hello,
I'm Dr. [redacted]
I am currently a[redacted]at the [redacted] specializing in geomorphology, glaciology, and geographic information technologies.Im working on a project about remote sensing and developed an application in parallel image processing for that reason I need a huge satelite image resource for testing my application. is it possible for you to Prepare it for me or test my attached application and send me feedback.
external application link
link to download
cheers.
--
Dr. [redacted]
Associate Professor [redacted]

40. The "link to download" in the email above redirected the recipient to malware hosted on a Dropbox account that was fraudulently registered in the name of VICTIM PERSON 2. The Conspirators used the same Conspirator email account that impersonated VICTIM PERSON 2 to send numerous spear phishing emails to multiple victims, including NASA, Lawrence Livermore National Laboratory, and VICTIM COMPANY 1.

41. On or about June 12, 2017, ARABI, using noreply@tleanalyser.com, sent a spear phishing email with a malicious link to one of VICTIM COMPANY 1's users, an organization that hosts satellite-tracking technology and information. The victim email address was one of the target email addresses that ESPARGHAM sent to ARABI on July 5, 2015, and the body of the email mirrored verbatim the content of the approximately 15 test spear phishing emails described above. The email appears below:

From: noreply@tleanalyser.com
To: [redacted]@[redacted].com>, [redacted]
Sent: Monday, 12 June, 2017 15:40:55
Subject: [redacted] Satellite Tracking Software

Hello dear

After months of hard work, we are delighted to officially announce the launch of our new and ultimate software for tracking satellite.
Our goal with this new software is to provide our visitors an easier way to track their desired satellite and also to allow the visitor the ability to conduct not only neighborhood searches but new developments and building specific searches. The new software is interactive and gives better access to conduct TLE and Map searches. Our current and prospective clients will find useful information about our services and recent production numbers on the homepage.

You can download our ultimate software from the link below:

http://www.tleanalyser.com/download.php

Kind regards
[redacted] Software Department
Contact Email: tleanalyser@gmail. com

The email also included a malicious link to tleanalyser.com, the above-described fraudulent website created by a member of the Conspiracy. When the recipient clicked on the malicious link in the June 12, 2017 email, an executable file was downloaded from tleanalyser.com to the recipient's computer. In addition, a member of the Conspiracy configured tleanalyser.com to automatically redirect visitors from the fraudulent website to VICTIM COMPANY 1's legitimate website so that so that potential victims would be less suspicious of the malicious link after clicking on it.

42. On or about June 12, 2017, ARABI sent a spear phishing email containing the same malicious link to an employee of VICTIM COMPANY 2, whose email address also appeared on the target list that ESPARGHAM sent to ARABI. An employee of VICTIM COMPANY 2 unwittingly clicked on the malicious link and forwarded the email to additional employees, who, in turn, also clicked on the malicious link, and thereby enabled the Conspirators to gain unauthorized access to VICTIM COMPANY 2's network.

43. The Conspirators then took further steps to infiltrate VICTIM COMPANY 2's networks:

a. On or about June 12, 2017, a member of the Conspiracy used a Metasploit Framework to install backdoors—a method to bypass normal authentication mechanisms—on various systems in VICTIM COMPANY 2's network. The Metasploit Framework is a tool that allows users to access compromised computers remotely.

b. On or about June 13, 2017, a member of the Conspiracy also deployed Mimikatz, a commonly used hacking tool used to steal credentials and modify administrative privileges, on compromised VICTIM COMPANY 2 servers.

c. In addition to the Metasploit Framework and Mimikatz, a member of the Conspiracy deployed three additional malicious programs in or around June 2017 and used them to gain and maintain access to VICTIM COMPANY 2's networks: NanoCore RAT, OCRA shell-code stagers, and Python Backdoor. The NanoCore RAT is a remote administration tool that allows the user to remotely administer computers and is used to record credentials and conduct surveillance using infected computers. The OCRA shell-code stagers are instructions that can be executed once malicious code is injected on a running system. The Python Backdoor is an additional way to control a victim's computer using the Python programming language.

d. Through these steps, the Conspirators successfully infected numerous VICTIM COMPANY 2 computers, including four Windows domain controllers, corporate IT cloud services, 16 servers, 69 laptops or workstations, and five terminal servers. Four of these infiltrated servers were physically located in the Eastern District of Virginia.

44. After compromising VICTIM COMPANY 2's networks, a member of the Conspiracy extracted data from one of VICTIM COMPANY 2's internal servers, information from an employee laptop, and information contained in cloud storage. Specifically, defendants ARABI and ESPARGHAM unlawfully obtained information relating to competitively sensitive business information, intellectual property, and vendor information valued in excess of $550,000.

45. The Conspirators compromised VICTIM COMPANY 1's networks as well. Among other evidence of the intrusion, in or about February 2017, a malicious file was discovered on VICTIM COMPANY 1 servers, which identified a group called IraNiaN DarK CoderS TeaM (IDC Team) and a domain, idc-team.net. Within the file identifying the group, the following message was embedded: "Hello IraNiaN DarK CoderS TeaM; Israel Fucked by M.R.S.CO and Ali.Pci." As discussed above, M.R.S.CO is a known alias of defendant ESPARGHAM, who leads the Iranian Dark Coders Team.

46. As a result of the breaches, VICTIM COMPANY 1 and VICTIM COMPANY 2 in the aggregate suffered losses in excess of $550,000.

(In violation of Title 18, United States Code, Section 371).

COUNT TWO

(Obtaining Information by Unauthorized Access to Protected Computers)

THE GRAND JURY FURTHER CHARGES:

47. The factual allegations contained in paragraphs 1 through 46 of this Indictment are repeated and realleged as if fully set forth herein.

48. On or about the following date, the defendants SAID POURKARIM ARABI and MOHAMMAD REZA ESPARGHAM attempted to intentionally access, and did intentionally access, without authorization, VICTIM COMPANY 2's protected computers in the Eastern District of Virginia, and thereby obtained information the value of which exceeded $5,000, and which offense was committed in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, and aided and abetted the same; to wit, ARABI and ESPARGHAM attempted to intentionally access, and did intentionally access, VICTIM COMPANY 2's protected computers located in the Eastern District of Virginia without authorization through various means including spear phishing, and aided and abetted the same, in furtherance of a wire fraud scheme to unlawfully transfer data from Victim Company 2's networks to ARABI and ESPARGHAM in violation of Title 18, United States Code, Section 1343, as follows:

Count	Date	Stolen Information
2	June 12, 2017	Competitively sensitive business information, intellectual property, and vendor information from VICTIM COMPANY 2 servers located in Manassas, Virginia

(In violation of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B)(ii) and (iii), and 2).

COUNTS THREE THROUGH SIX

(Intentional Damage to Protected Computers)

THE GRAND JURY FURTHER CHARGES THAT:

49. The allegations contained in paragraphs 1 through 46 of this Indictment are repeated and realleged as if fully set forth herein.

50. From at least on or about the following dates, the defendants SAID POURKARIM ARABI and MOHAMMAD REZA ESPARGHAM knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and aided and abetted the same; and, through such conduct, intentionally caused damage without authorization to VICTIM COMPANY 2's protected computers in the Eastern District of Virginia and thereby caused loss to one or more persons during a one-year period, from the defendants' course of conduct affecting protected computers, aggregating at least $5,000 in value, as follows:

Count	Date	Description of Transmissions
3	June 12 – 29, 2017	Deployment of malware to Server 1 belonging to VICTIM COMPANY 2 and located in Manassas, Virginia
4	June 12 – 29, 2017	Deployment of malware to Server 2 belonging to VICTIM COMPANY 2 and located in Manassas, Virginia
5	June 12 – 29, 2017	Deployment of malware to Server 3 belonging to VICTIM COMPANY 2 and located in Manassas, Virginia
6	June 12 – 29, 2017	Deployment of malware to Server 4 belonging to VICTIM COMPANY 2 and located in Manassas, Virginia

(In violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(B), and 2).

COUNTS SEVEN AND EIGHT
(Aggravated Identity Theft)

THE GRAND JURY FURTHER CHARGES THAT:

51. The factual allegations contained in paragraphs 1 through 46 of this Indictment are repeated and realleged as if fully set forth herein.

52. From at least on or about the following dates, in the Eastern District of Virginia and elsewhere, SAID POURKARIM ARABI 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, 1028A(c), and aided and abetted the same; to wit, ARABI knowingly transferred, possessed, and used, and aided and abetted the transfer, possession, and use of the names and employment information of identity theft victims during and in relation to each of the computer fraud offenses charged in Counts One through Six of this Indictment, as follows:

7	May 26, 2017 through October 9, 2017	The use of the VICTIM PERSON 1's name and former employer to purchase fraudulent domains, and hacking tools used in the network compromise of VICTIM COMPANY 1 and VICTIM COMPANY 2.
8	September 17, 2016 through January 3, 2018	The use of VICTIM PERSON 2's name, title, and employer to send spear phishing emails.

(In violation of Title 18, United States Code, Sections 1028A and 2).

COUNT NINE
(Conspiracy to Commit Wire Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

53. The factual allegations contained in paragraphs 1 through 46 of this Indictment are repeated and realleged as if fully set forth herein.

54. From on or about May 2016 through on or about at least February 2019, defendants SAID POURKARIM ARABI, MOHAMMAD REZA ESPARGHAM, and MOHAMMAD BAYATI, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit wire fraud in violation of Title 18, United States Code, Section 1343.

55. It was part and object of the Conspiracy that ARABI, ESPARGHAM, and BAYATI, the defendants, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud U.S. persons and entities involved in aerospace and satellite technology, and to obtain property by means of materially 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 to defraud, in violation of Title 18, United States Code, Section 1343.

(In violation of Title 18, United States Code, Section 1349).

FORFEITURE NOTICE

THE GRAND JURY FINDS PROBABLE CAUSE FOR FORFEITURE AS DESCRIBED BELOW:

56. Pursuant to Fed. R. Crim. P. 32.2(a), the defendants are hereby noticed that if convicted of any of the offenses alleged in Counts One through Six of this Indictment, SAID POURKARIM ARABI, MOHAMMAD REZA ESPARGHAM, and MOHAMMAD BAYATI, the defendants, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 1030(i), their interest in any personal property used or intended to be used to commit or to facilitate the commission of such offense; and any property, real or personal, constituting or derived from, any proceeds they obtained, directly or indirectly, as a result of such offense. The defendants are further notified that if convicted of the offense alleged in Count Nine of this Indictment, 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 property, real and personal, which constitutes or is derived from proceeds traceable to the commission of the offense.

(Pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 1030(i) and Title 28, United States Code Section 2461(c)).

Pursuant to the E-Government Act,, The original of this page has been filed under seal in the Clerk's Office

Foreperson of the Grand Jury

G. ZACHARY TERWILLIGER
UNITED STATES ATTORNEY

Nathaniel Smith III
Jay V. Prabhu
Danya E. Atiyeh
Assistant United States Attorneys

Evan N. Turgeon
Trial Attorney
National Security Division, U.S. Department of Justice