ORIGINAL

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
- - - - - - - - - - - - - - - - - - - -x

UNITED STATES OF AMERICA	:	**SEALED INDICTMENT**
- v. -	:	16 Cr. 16 CRIM 48
AHMAD FATHI, HAMID FIROOZI, AMIN SHOKOHI, SADEGH AHMADZADEGAN, a/k/a "Nitr0jen26," OMID GHAFFARINIA, a/k/a "PLuS," SINA KEISSAR, and NADER SAEDI, a/k/a "Turk Server,"	:	
Defendants.	:	

- - - - - - - - - - - - - - - - - - - -x

USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #:
DATE FILED: 1/21/16

COUNT ONE

(CONSPIRACY TO COMMIT COMPUTER HACKING - ITSEC TEAM)

The Grand Jury charges:

BACKROUND ON THE DEFENDANTS AND RELATED ENTITIES

1. At all times relevant to this Indictment, ITSec Team and Mersad Co. ("Mersad") were private computer security companies based in the Islamic Republic of Iran ("Iran") that performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps ("IRGC"), which is one of several entities within the Iranian Government responsible for Iranian intelligence.

2. At certain times relevant to this Indictment, AHMAD FATHI, HAMID FIROOZI, and AMIN SHOKOHI, the defendants

(collectively, the "ITSec Team Defendants"), were experienced computer hackers who worked for ITSec Team.

3. At certain times relevant to this Indictment, SADEGH AHMADZADEGAN, a/k/a "Nitr0jen26," OMID GHAFFARINIA, a/k/a "PLuS," SINA KEISSAR, and NADER SAEDI, a/k/a "Turk Server," the defendants (collectively, the "Mersad Defendants"), were experienced computer hackers who worked for Mersad.

BACKGROUND ON DDoS ATTACKS

4. In general, a distributed denial of service ("DDoS") attack is a type of cyberattack in which a malicious actor seeks to overwhelm and thereby disable the victim's Internet-accessible computer servers through one of several means.

5. In preparing for a DDoS attack, the malicious actor typically compromises and gains remote control of computers and computer servers by placing malicious software, or malware, on them. The malicious actor often collects hundreds or thousands of such compromised computers and servers (which are described individually as "bots" and collectively as a "botnet"). Once the malicious actor has gained control over the botnet, he can direct the computers or servers comprising the botnet to carry out computer network attack and computer network exploitation activity, including DDoS attacks.

6. In conducting a DDoS attack, the malicious actor can, for example, remotely command the botnet to flood the victim server with electronic communications in order to overwhelm the server's resources. As a result of this type of DDoS attack, the victim server becomes unable to receive and maintain connections from legitimate Internet traffic, and is thereby disabled during the duration of the attack.

THE U.S. FINANCIAL INDUSTRY DDoS ATTACKS

7. At certain times relevant to this Indictment, the ITSec Team Defendants and Mersad Defendants conducted extensive computer network exploitation and computer network attacks against victim corporations in the United States. These included, among other things, a large-scale coordinated campaign of DDoS attacks against U.S. financial institutions and other corporations in the financial sector, including institutions based in the Southern District of New York (the "U.S. Financial Industry DDoS Attacks"), intended to undermine the business of those companies. In particular, through the U.S. Financial Industry DDoS Attacks, the defendants variously disabled and attempted to disable computer servers belonging to these corporations in an effort to prevent the corporations from conducting business with customers online during the course of the attacks, including, among other things, providing online banking services and other information to customers.

computer network infrastructure. The attacks were coordinated in timing, targets, technique and nature.

THE ITSEC TEAM CYBER INTRUSIONS AND DDOS ATTACKS

10. Starting at least in or about December 2011, up to and including at least in or about December 2012, AHMAD FATHI, HAMID FIROOZI, and AMIN SHOKOHI, the defendants, and their co-conspirators planned and executed certain of the U.S. Financial Industry DDoS Attacks, including DDoS attacks targeting Bank of America, N.A. ("Bank of America"), NASDAQ, New York Stock Exchange ("NYSE"), Capital One Bank, N.A. ("Capital One"), ING Bank, Branch Banking and Trust Company ("BB&T"), Fidelity National Information Services, U.S. Bank, N.A. ("U.S. Bank"), and PNC Bank. In addition, as set forth below, FATHI, FIROOZI, SHOKOHI, and their co-conspirators carried out a series of DDoS attacks against AT&T, Inc. ("AT&T") in or about August 2012.

The ITSec Team Defendants

11. At all times relevant to this Indictment, AHMAD FATHI, the defendant, was the leader of the ITSec Team Defendants. In that capacity, among other things, FATHI was responsible for supervising and coordinating ITSec Team's participation in the DDoS attacks against the U.S. financial sector and AT&T. As the leader of ITSec TEAM, FATHI was

responsible for managing computer intrusion and cyberattack projects being conducted on behalf of the Government of Iran.

12. At certain times relevant to this Indictment, HAMID FIROOZI, the defendant, was a network manager at ITSec Team. In that role, as set forth below, FIROOZI procured computer servers in the United States and elsewhere for ITSec Team's botnet that were used to coordinate and direct the U.S. Financial Industry DDoS Attacks.

13. At certain times relevant to this Indictment, AMIN SHOKOHI, the defendant, was a computer hacker who worked for ITSec Team. Among other things, SHOKOHI helped to build the ITSec Team botnet used in the U.S. Financial Industry DDoS Attacks, and created malware used to direct the botnet to engage in those attacks. During the time in which he worked in support of the U.S. Financial Industry DDoS Attacks, SHOKOHI received credit for his computer intrusion work from the Iranian Government towards completion of his mandatory military service in Iran.

Means and Methods of the Conspiracy With Respect to ITSec Team's U.S. Financial Industry DDoS Attacks

14. AHMAD FATHI, HAMID FIROOZI, and AMIN SHOKOHI, the defendants, and their co-conspirators planned and participated in the U.S. Financial Industry DDoS Attacks against the victims listed above as follows:

a. Among other things, with FATHI's knowledge, SHOKOHI and other co-conspirators built the ITSec Team botnet used in the DDoS attacks of the victim institutions. Specifically, by scanning the Internet, they identified computers and computer servers running versions of popular website content management software that had not been updated to address certain known security vulnerabilities. FATHI, SHOKOHI, and other co-conspirators subsequently obtained unauthorized access to thousands of such computers and computer servers, some of which were located within the United States. Thereafter, the co-conspirators installed on the compromised computers and computer servers malicious software authored by SHOKOHI and others which gave them remote access to, and control of, these compromised machines, which together constituted the ITSec Team botnet used in the U.S. Financial Industry DDoS Attacks and the DDoS attacks targeting AT&T.

b. In addition to building the botnet, FATHI, SHOKOHI, and their co-conspirators authored and obtained malicious computer scripts that were designed to cause computers to execute specific types of DDoS attacks ("attack scripts"), and installed them on the compromised computers within the ITSec Team botnet used to execute the DDoS attacks.

c. To coordinate the botnet's activity, FIROOZI directed others to lease computer servers in the United States

and elsewhere, servers which FIROOZI and FATHI could then access and control, to serve as "command and control" or "C2" servers for the DDoS attacks. The C2 servers transmitted commands to the compromised computers within the ITSec Team botnet to execute the attack scripts in order to overwhelm and disable the targeted victim computer servers. Further, and among other things, the defendants and their co-conspirators used these C2 servers to perform online surveillance of victims' servers prior to the attacks, and to monitor the impact of the attacks on the victims' servers.

STATUTORY ALLEGATIONS

15. From at least in or about December 2011, up to and including at least in or about December 2012, in the Southern District of New York and elsewhere, AHMAD FATHI, HAMID FIROOZI, and AMIN SHOKOHI, the defendants, who will first be brought to the Southern District of New York, and others known and unknown, willfully and knowingly, combined, conspired, confederated, and agreed together and with each other to engage in computer hacking, and to aid and abet the same, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 2.

16. It was a part and an object of the conspiracy that AHMAD FATHI, HAMID FIROOZI, and AMIN SHOKOHI, the defendants, and others known and unknown, willfully and 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 would and did cause a loss (including loss resulting from a related course of conduct affecting one and more other protected computers) aggregating to at least $5,000 to one and more persons during any one year period and caused damages affecting ten or more protected computers during any one year period, and would and did aid and abet such unauthorized access, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i), (c)(4)(A)(i)(I), (c)(4)(A)(i)(VI) and 2.

(Title 18, United States Code, Sections 1030(b) and 2; Title 18, United States Code, Section 3238.)

COUNT TWO

(CONSPIRACY TO COMMIT COMPUTER HACKING - MERSAD)

The Grand Jury further charges:

17. The allegations in paragraphs 1 and 3 through 9 of this Indictment are repeated and realleged as though fully set forth herein.

THE MERSAD DDOS ATTACKS

18. As set forth below, from at least in or about September 2012, up to and including at least in or about May 2013, the Mersad Defendants and their co-conspirators participated in the U.S. Financial Industry DDoS Attacks. In

particular, as described below, the Mersad Defendants and their co-conspirators executed approximately 150 days of coordinated DDoS attacks against at least approximately 24 U.S. financial-sector corporations, including Ally Bank, American Express, Ameriprise, Bank of America, Bank of Montreal, BB&T, Banco Nilbao Vizyana Argentaria ("BBVA"), Capital One, J.P. Morgan Chase Bank, Citibank, N.A., Citizens Bank, Fifth Third Bank, FirstBank, HSBC, Key Bank, NYSE, PNC, Regions Bank, State Street Bank, SunTrust Bank, Union Bank, N.A., US Bank, Wells Fargo, and Zions First National Bank.

Background on Mersad and the Mersad Defendants

19. Mersad was founded in or about early 2011 by members of Iran-based computer hacking groups Sun Army and Ashiyane Digital Security Team ("ADST"), including SADEGH AHMADZADEGAN, a/k/a "Nitr0jen26," and OMID GHAFFARINIA, a/k/a "PLuS," the defendants. Sun Army and ADST have publicly claimed responsibility for performing network attacks on computer servers of the United States Government, and ADST has publicly claimed to perform computer hacking work on behalf of the Government of Iran. As Sun Army members, AHMADZADEGAN and GHAFFARINIA claimed responsibility for hacking into computer servers belonging to the National Aeronautics and Space Administration ("NASA"), and the defacement of approximately nine NASA websites in or about February 2012.

20. At all relevant times, in addition to being a co-founder of Mersad, and a computer hacker associated with Sun Army and ADST, SADEGH AHMADZADEGAN, a/k/a "Nitr0jen26," the defendant, was responsible for managing the Mersad botnet used in the U.S. Financial Industry DDoS Attacks. AHMADZADEGAN also provided training to Iranian intelligence personnel.

21. At all relevant times, in addition to being a co-founder of Mersad, and a former computer hacker with Sun Army and ADST, OMID GHAFFARINIA, a/k/a "PLuS," the defendant, created malicious computer code that remotely compromised computer servers to support building the Mersad botnet which was used to conduct computer network intrusions and cyberattacks, including the U.S. Financial Industry DDoS Attacks. GHAFFARINIA has also claimed to have successfully performed computer intrusions on thousands of computer servers based in the United States, the United Kingdom, and Israel.

22. At all relevant times, NADER SAEDI, a/k/a "Turk Server," the defendant, was an employee of Mersad and a former computer hacker with Sun Army who has expressly touted himself as an expert in DDoS attacks. As an employee of Mersad, SAEDI wrote computer scripts used to locate and exploit vulnerable servers to help build the Mersad botnet used in the U.S. Financial Industry DDoS Attacks.

23. At all relevant times, SINA KEISSAR, the defendant, was an employee of Mersad. In that capacity, KEISSAR procured U.S.-based computer servers used by Mersad to access and manipulate the Mersad botnet used in the U.S. Financial Industry DDoS attacks. KEISSAR also performed preliminary testing of the same botnet prior to its use in the U.S. Financial Industry DDoS Attacks.

Means and Methods of the Conspiracy

24. SADEGH AHMADZADEGAN, a/k/a "Nitr0jen26," OMID GHAFFARINIA, a/k/a "PLuS," NADER SAEDI, a/k/a "Turk Server," and SINA KEISSAR, the defendants, and their co-conspirators planned and assisted in the U.S. Financial Industry DDoS Attacks against the victims listed above as follows:

a. AHMADZADEGAN, GHAFFARINIA, SAEDI, KEISSAR, and their co-conspirators built the Mersad botnet by obtaining unauthorized access to, and compromising, thousands of computers and computer servers, some of which were located in the United States. AHMADZADEGAN, GHAFFARINIA, SAEDI, and KEISSAR also developed malware and computer scripts which they installed on the compromised computers and computer servers that constituted the Mersad botnet, which allowed for remote access and control of the compromised computers.

b. Thereafter, AHMADZADEGAN, GHAFFARINIA, SAEDI, and KEISSAR placed malicious computer scripts on the

things, information regarding water levels and temperature, and the status of the sluice gate, which is responsible for controlling water levels and flow rates. Although access to the SCADA system typically would have also permitted FIROOZI to remotely operate and manipulate the sluice gate on the Bowman Dam, unbeknownst to FIROOZI, the sluice gate control had been manually disconnected for maintenance issues prior to the time FIROOZI gained access to the systems.

STATUTORY ALLEGATION

28. From at least on or about August 28, 2013, and on or about September 18, 2013, in the Southern District of New York, and elsewhere, HAMID FIROOZI, the defendant, willfully and intentionally accessed a protected computer without authorization, and as a result of such conduct, would and did recklessly cause damage, and would and did aid and abet the same, which would and did cause a loss (including loss resulting from a related course of conduct affecting one or more other protected computers) aggregating to at least $5,000 in value during any one year period, and would and did attempt to cause a threat to public health or safety, to wit, FIROOZI, from a computer in Iran, accessed without authorization the SCADA system for the Bowman Dam, a dam located in Rye, New York, and obtained information regarding the status and operation of

controls for the dam, and caused over $30,000 in remediation costs.

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

FORFEITURE ALLEGATION

29. As a result of committing one or more of the offenses alleged in Counts One through Three of this Indictment, AHMAD FATHI, HAMID FIROOZI, AMIN SHOKOHI, SADEGH AHMADZADEGAN, a/k/a "Nitr0jen26," OMID GHAFFARINIA, a/k/a "PLuS," NADER SAEDI, a/k/a "Turk Server," and SINA KEISSAR, the defendants, shall forfeit to the United States, pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i)(1), the defendants' interests in any personal property that was used or intended to be used to commit or facilitate the commission of such offenses, and any property constituting, or derived from, proceeds obtained directly or indirectly as a result of one or both of the said offenses, including but not limited to a sum of money representing the amount of proceeds obtained as a result of one or both of the said offenses.

SUBSTITUTE ASSETS PROVISION

30. 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 18 U.S.C. § 982(b)(1) and 21 U.S.C. § 853(p), to seek forfeiture of any other property of said defendants up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 982(a)(2)(B) and (b)(1), and Title 21, United States Code, Section 853(p).)

FOREPERSON

PREET BHARARA
United States Attorney

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

AHMAD FATHI,
HAMID FIROOZI,
AMIN SHOKOHI,
SADEGH AHMADZADEGAN,
a/k/a "Nitr0jen26,"
OMID GHAFFARINIA,
a/k/a "PLuS,"
SINA KEISSAR, and
NADER SAEDI,
a/k/a "Turk Server,"

Defendants.

INDICTMENT

16 Cr.

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

PREET BHARARA
United States Attorney.

A TRUE BILL

Yolanda Ocasio
Foreperson.

January 21, 2016
Filed Sealed Indictment.
U.S.M.J. Debra Freeman