JSH/WAH/2016R00103

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon.
	:	
v.	:	Criminal No. 18 - CR - 704 (BRM)
	:	
FARAMARZ SHAHI SAVANDI and	:	18 U.S.C. § 371
MOHAMMAD MEHDI SHAH	:	18 U.S.C. § 1030(a)(5)(A)
MANSOURI	:	18 U.S.C. § 1030(a)(7)(C)
	:	18 U.S.C. § 1349

INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges:

COUNT 1
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers)

1. At all times relevant to Count 1 of this Indictment:

The Defendants

a. Defendant FARAMARZ SHAHI SAVANDI was a computer hacker who resided in Iran.

b. Defendant MOHAMMAD MEHDI SHAH MANSOURI was a computer hacker who resided in Iran.

Relevant Individuals and Entities

c. Exchanger #1 was a Bitcoin exchanger based in Iran.

d. Exchanger #2 was a Bitcoin exchanger based in Iran.

e. European VPS #1 was a virtual private server hosted in

Europe.

f. European VPS #2 was a virtual private server hosted in Europe.

Victims

g. Allscripts Healthcare Solutions, Inc. was a company headquartered in Chicago, Illinois that provided physician practices, hospitals, and other healthcare providers with practice management and electronic health record technology.

h. The City of Atlanta was the capital of Georgia, with a population of over 480,000 residents.

i. The City of Newark was a municipality in New Jersey, with a population of over 280,000 residents.

j. The Colorado Department of Transportation was headquartered in Denver, Colorado, and administered Colorado's state government transportation responsibilities.

k. Hollywood Presbyterian Medical Center was a hospital located in Los Angeles, California.

l. Kansas Heart Hospital was a hospital located in Wichita, Kansas.

m. Laboratory Corporation of America Holdings, more commonly known as LabCorp, was a company headquartered in Burlington,

North Carolina that operated one of the largest clinical laboratory networks in the world, with a United States network of 36 primary laboratories.

n. MedStar Health was a healthcare organization headquartered in Columbia, Maryland that operated more than 120 entities, including ten hospitals in the Baltimore–Washington metropolitan area.

o. The Mercer County Business was a business located in Mercer County, New Jersey.

p. Nebraska Orthopedic Hospital was a hospital located in Omaha, Nebraska, now known as OrthoNebraska Hospital.

q. The Port of San Diego was a public-benefit corporation headquartered in San Diego, California that administered two marine cargo facilities on San Diego Bay.

r. The University of Calgary was a university located in Calgary, Alberta, Canada.

Overview

2. From in or about December 2015 to the present, FARAMARZ SHAHI SAVANDI and MOHAMMAD MEHDI SHAH MANSOURI (collectively, "Defendants") engaged in an international computer hacking and extortion scheme, whereby they:

a. Used sophisticated techniques and tools to hack into the computer networks of hospitals, schools, companies, government agencies, and

other entities, primarily located in the United States, including the victims set forth in paragraphs 1(g) through 1(r) (the "Victims");

b. Encrypted computers on the Victims' networks, using a form of malicious software created by Defendants called SamSam Ransomware, with the objective of crippling the Victims by preventing them from accessing or using data on the compromised computers, thus forcing many Victims to shut down or dramatically curtail their operations; and

c. Extorted the Victims for ransom payments in exchange for the decryption keys to unlock the compromised computers.

3. The defendants hacked, encrypted, and extorted more than 200 Victims, and collected more than $6 million in ransom payments. The Victims incurred additional losses exceeding $30 million resulting from the loss of access to their data.

Relevant Terms

4. Bitcoin was a type of virtual currency, circulated over the Internet as a form of value. Bitcoin were not issued by any government, bank, or company, but rather were generated and controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin were just one of many varieties of virtual currency.

5. "Bitcoin addresses" were the particular virtual locations to which Bitcoin were sent and received. A Bitcoin address was analogous to a bank

account number and was represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each Bitcoin address was controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address's private key could authorize a transfer of Bitcoin from that address to another Bitcoin address.

6. "Bitcoin exchangers" were persons in the business of exchanging fiat currency (currency that derives its value from government regulation or law, such as the U.S. dollar or the Iranian rial) for Bitcoin, and exchanging Bitcoin for fiat currency.

7. "Encryption" was the translation of data into a secret code. In order to access encrypted data, a user had to have access to a password (known as a "decryption key") that enabled the user to decrypt it.

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

9. "Ransomware" was a type of malware that infected a computer and encrypted some or all of the data on the computer. Distributors of ransomware typically extorted the user of the encrypted computer by demanding that the user pay a ransom in order to decrypt and recover the data on the computer.

10. "SamSam Ransomware" was a form of sophisticated malware that encrypted victim computers. SamSam Ransomware has also been given other names by security researchers, such as "Samas Ransomware" and "MSIL/SAMAS.A Ransomware." The process of encrypting victim computers with SamSam Ransomware required the execution of the malicious code by the distributor of the malware (i.e., direct human interaction). Once data on a computer was encrypted, distributors of the malware could then extort victims by demanding a ransom in exchange for the decryption key for the encrypted data.

11. "Security vulnerabilities" were unintended flaws in software code or an operating system that left a computer open to exploitation in the form of unauthorized access or malicious behavior, such as the deployment of malware.

12. A "server" was a type of computer or device on a network that managed network resources. A "virtual private server," or VPS, was a virtual server that a user perceived as a single physical server, even though it was installed on a physical server potentially running multiple operating systems.

13. Tor was a computer network designed to facilitate anonymous communication over the Internet. The Tor network did this by routing a user's communications through a globally distributed network of relay computers, or proxies, rendering ineffective any conventional Internet Protocol ("IP") address-

based methods of identifying users. To access the Tor network, a user installed specific Tor software. The Tor network also enabled users to operate hidden sites that operate similarly to conventional websites.

The Conspiracy

14. From in or about December 2015 through in or about November 2018, in Essex and Mercer Counties, in the District of New Jersey, and elsewhere, defendants

FARAMARZ SHAHI SAVANDI and
MOHAMMAD MEHDI SHAH MANSOURI

did knowingly and intentionally conspire and agree 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, and cause loss to persons during a 1-year period from Defendants' course of conduct affecting protected computers aggregating at least $5,000 in value, and cause damage affecting 10 or more protected computers during a 1-year period, contrary to Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B); and,

b. to knowingly and with intent to extort from any person any money or other thing of value, transmit in interstate and foreign commerce any communication containing a demand and request for money and other thing of

value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, contrary to Title 18, United States Code, Sections 1030(a)(7)(C) and (c)(3)(A).

Goal of the Conspiracy

15. The goal of the conspiracy was for Defendants, acting from inside Iran, to enrich themselves by: (a) authoring malware (i.e., the SamSam Ransomware) that would, when executed, encrypt data on Victim computers; (b) conducting reconnaissance and research to select and target potential Victims; (c) accessing Victim computers without authorization through security vulnerabilities; (d) installing and executing the SamSam Ransomware on Victim computers, resulting in the encryption of data on the computers; (e) extorting Victims by demanding a ransom paid in Bitcoin in exchange for decryption keys for the encrypted data; and (f) collecting ransom payments from Victims that paid the ransom.

Manner and Means of the Conspiracy

16. It was part of the conspiracy that:

a. Defendants authored various versions of the SamSam Ransomware, which was designed to encrypt data on Victim computers. SamSam Ransomware was designed to maximize the damage caused to the Victim by, for instance, also encrypting backups of the targeted computers. Defendants created the first operational version of SamSam in or about

December 2015. Since then, Defendants have regularly updated and refined the SamSam Ransomware. For instance, Defendants added more sophisticated encryption to the SamSam Ransomware to make it more difficult to analyze.

b. Defendants hacked into (i.e., accessed without authorization) the computer networks of the Victims, both inside and outside the United States. They also conducted online research in order to select and target potential victims. Defendants used a variety of methods to gain access to Victim computer networks, including exploiting known security vulnerabilities in common server software and utilizing virtual private servers such as European VPS #1 and European VPS #2 to mask their identities.

c. Once inside a Victim's computer network, Defendants used sophisticated hacking techniques and tools to conduct reconnaissance and expand their access to the Victim computer networks. Among other things, Defendants scanned a Victim's computer network to identify computers to target for encryption. Early in the conspiracy, this reconnaissance often lasted for weeks. Over time, Defendants moved more quickly from hacking into a Victim's network to deploying the SamSam Ransomware. For instance, by in or about 2018, Defendants sometimes deployed the SamSam Ransomware within hours of hacking into a Victim's computer network.

d. After conducting reconnaissance, Defendants installed the

SamSam Ransomware on as many computers within the Victim network as possible. Once the SamSam Ransomware was widely deployed within the Victim's computer network, Defendants then executed the malware to encrypt computers on the Victim network. This coordinated encryption attack, which was disguised to appear like legitimate network activity, was usually launched outside regular business hours, when a Victim would find it more difficult to mitigate the attack.

e. The simultaneous, mass encryption of a Victim's computers was intended to—and often did—cripple the regular business operations of the Victims. Without use of their data, most Victims were unable to function normally; many had to shut down or drastically curtail their operations. These devastating attacks often caused substantial losses to the Victims.

f. Defendants extorted Victims by leaving a ransom note in the form of a file on each computer encrypted by SamSam Ransomware. Each Victim's ransom note told the Victim that its files were encrypted, told the Victim that it would have to pay Bitcoin to get the decryption keys, and directed the Victim to a webpage to communicate with Defendants (the "Ransom Webpage"). The ransom notes usually threatened to permanently delete the decryption keys for the Victim's computers after seven days. For instance, on or about April 25, 2017, Defendants encrypted computers

belonging to the City of Newark, and left behind a ransom note. A copy of that ransom note is shown at Attachment A.

g. Defendants created a Ransom Webpage for each Victim. Early in the conspiracy, Defendants created the Ransom Webpages at a public provider. Later in the conspiracy, Defendants created Ransom Webpages hidden by the Tor network, and instructed Victims to install specific Tor software, and then navigate to a hidden Tor page. Defendants used the Ransom Webpages to communicate with Victims, arrange for payment, and provide decryption keys to Victims that paid the ransom. To spur prompt payment, the Ransom Webpages often included a threatening timer clock after which a Victim's decryption keys would be deleted. For instance, on or about March 22, 2018, Defendants encrypted computers belonging to the City of Atlanta, and directed the Victim to a Ransom Webpage created specifically for that attack. A copy of that Ransom Webpage is shown at Attachment B.

h. Defendants collected payments in Bitcoin from Victims that paid the ransom. Although the value of Bitcoin fluctuates, measured at the time the ransoms were paid, Defendants successfully extorted more than $6 million from Victims. Defendants periodically exchanged the accumulated Bitcoin proceeds into Iranian rial using Bitcoin exchangers, including Exchanger #1 and Exchanger #2.

Overt Acts

17. In furtherance of the conspiracy and to effect its unlawful object, Defendants committed and caused to be committed the following overt acts in the District of New Jersey and elsewhere:

a. In or about December 2015, Defendants authored the first version of the SamSam Ransomware.

b. On or about December 14, 2015, Defendants exchanged multiple chat communications discussing the development and functionality of the SamSam Ransomware.

c. On or about January 11, 2016, Defendants accessed the computer network of the Mercer County Business in New Jersey and deployed the SamSam Ransomware on its computers, encrypting them, all without authorization.

d. On or about January 11, 2016, Defendants extorted the Mercer County Business in New Jersey by demanding a ransom paid in Bitcoin in exchange for decryption keys for the encrypted data.

e. On or about February 5, 2016, Defendants accessed the computer network of Hollywood Presbyterian Medical Center and deployed the SamSam Ransomware on its computers, encrypting them, all without authorization.

f. On or about February 5, 2016, Defendants extorted

Hollywood Presbyterian Medical Center by demanding a ransom paid in Bitcoin in exchange for decryption keys for the encrypted data.

g. On or about February 18, 2016, Defendants exchanged multiple chat communications in which they agreed to equally divide ransom proceeds.

h. On or about March 8, 2016, defendant MANSOURI and Exchanger #2 exchanged multiple chat communications discussing Bitcoin.

i. On or about March 10, 2016, defendant MANSOURI received a chat communication from Exchanger #2 concerning Bitcoin.

j. On or about March 27, 2016, Defendants accessed the computer network of MedStar Health and deployed the SamSam Ransomware on its computers, encrypting them, all without authorization.

k. On or about March 27, 2016, Defendants extorted MedStar Health by demanding a ransom paid in Bitcoin in exchange for decryption keys for the encrypted data.

l. On or about May 15, 2016, Defendants paid for the use of European VPS #1.

m. On or about May 15, 2016, Defendants searched for the term "kansasheart.com" on an online search engine.

n. On or about May 15, 2016, Defendants accessed the publicly-accessible website of Kansas Heart Hospital.

o. On or about May 18, 2016, Defendants accessed the computer network of Kansas Heart Hospital and deployed the SamSam Ransomware on its computers, encrypting them, all without authorization.

p. On or about May 18, 2016, Defendants extorted Kansas Heart Hospital by demanding a ransom paid in Bitcoin in exchange for decryption keys for the encrypted data.

q. On or about May 19, 2016, Defendants paid for the use of European VPS #2.

r. On or about May 27, 2016, Defendants, utilizing in part European VPS #1 and European VPS #2, accessed the computer network of the University of Calgary and deployed the SamSam Ransomware on its computers, encrypting them, all without authorization.

s. On or about May 27, 2016, Defendants extorted the University of Calgary by demanding a ransom paid in Bitcoin in exchange for decryption keys for the encrypted data.

t. On or about May 28, 2016, Defendants exchanged multiple chat communications discussing the attack on, and extortion of, the University of Calgary.

u. On or about July 21, 2016, Defendants exchanged multiple chat communications discussing the conversion of accumulated Bitcoin into Iranian rial.

v. On or about July 21, 2016, defendant MANSOURI sent a chat communication to Exchanger #1 instructing him to convert Bitcoin associated with ransom proceeds into Iranian rial and to deposit the rial into accounts controlled by defendant MANSOURI and defendant SAVANDI.

w. On or about July 21, 2016, defendant MANSOURI received a chat communication from Exchanger #1 confirming the conversion of Bitcoin associated with ransom proceeds into Iranian rial and the deposit thereof into accounts controlled by defendant MANSOURI and defendant SAVANDI.

x. On or about July 28, 2016, Defendants, utilizing in part European VPS #2, accessed the computer network of Nebraska Orthopedic Hospital and deployed the SamSam Ransomware on its computers, encrypting them, all without authorization.

y. On or about July 28, 2016, Defendants extorted Nebraska Orthopedic Hospital by demanding a ransom paid in Bitcoin in exchange for decryption keys for the encrypted data.

z. On or about August 12, 2016, defendant MANSOURI sent a chat communication to Exchanger #1 instructing him to convert Bitcoin associated with ransom proceeds into Iranian rial and to deposit the rial into accounts controlled by defendant MANSOURI and defendant SAVANDI.

aa. On or about August 12, 2016, defendant MANSOURI received a chat communication from Exchanger #1 confirming the conversion

of Bitcoin associated with ransom proceeds into Iranian rial and the deposit thereof into accounts controlled by defendant MANSOURI and defendant SAVANDI.

bb. On or about April 25, 2017, Defendants accessed the computer network of the City of Newark in New Jersey and deployed the SamSam Ransomware on computers belonging to the entity, encrypting them, all without authorization.

cc. On or about April 25, 2017, Defendants extorted the City of Newark in New Jersey by demanding a ransom paid in Bitcoin in exchange for decryption keys for the encrypted data.

dd. In or about June 2017, Defendants authored an updated, refined version of the SamSam Ransomware.

ee. In or about October 2017, Defendants authored a further updated, refined version of the SamSam Ransomware.

ff. On or about January 18, 2018, Defendants accessed the computer network of Allscripts Healthcare Solutions, Inc. and deployed the SamSam Ransomware on its computers, encrypting them, all without authorization.

gg. On or about January 18, 2018, Defendants extorted Allscripts Healthcare Solutions, Inc. by demanding a ransom paid in Bitcoin in exchange for decryption keys for the encrypted data.

hh. On or about February 5, 2018, defendant SAVANDI received funds associated with ransom proceeds, which were converted into Iranian rial and deposited by Exchanger #2.

ii. On or about February 10, 2018, defendant MANSOURI received funds associated with ransom proceeds, which were converted into Iranian rial and deposited by Exchanger #2.

jj. On or about February 18, 2018, defendant SAVANDI received funds associated with ransom proceeds, which were converted into Iranian rial and deposited by Exchanger #2.

kk. On or about February 19, 2018, Defendants accessed the computer network of the Colorado Department of Transportation and deployed the SamSam Ransomware on its computers, encrypting them, all without authorization.

ll. On or about February 19, 2018, Defendants extorted the Colorado Department of Transportation by demanding a ransom paid in Bitcoin in exchange for decryption keys for the encrypted data.

mm. On or about March 22, 2018, Defendants accessed the computer network of the City of Atlanta and deployed the SamSam Ransomware on computers belonging to the entity, encrypting them, all without authorization.

nn. On or about March 22, 2018, Defendants extorted the City of

Atlanta by demanding a ransom paid in Bitcoin in exchange for decryption keys for the encrypted data.

oo. On or about April 19, 2018, defendant SAVANDI received funds associated with ransom proceeds, which were converted into Iranian rial and deposited by Exchanger #2.

pp. On or about July 14, 2018, Defendants accessed the computer network of LabCorp and deployed the SamSam Ransomware on its computers, encrypting them, all without authorization.

qq. On or about July 14, 2018, Defendants extorted LabCorp by demanding a ransom paid in Bitcoin in exchange for decryption keys for the encrypted data.

rr. On or about September 25, 2018, Defendants accessed the computer network of the Port of San Diego and deployed the SamSam Ransomware on its computers, encrypting them, all without authorization.

ss. On or about September 25, 2018, Defendants extorted the Port of San Diego by demanding a ransom paid in Bitcoin in exchange for decryption keys for the encrypted data.

All in violation of Title 18, United States Code, Section 371.

COUNT 2
(Conspiracy to Commit Wire Fraud)

1. The allegations contained in paragraphs 1 through 13, 16, and 17 of Count 1 of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. From in or about December 2015 through in or about November 2018, in Essex and Mercer Counties, in the District of New Jersey, and elsewhere, defendants

FARAMARZ SHAHI SAVANDI and
MOHAMMAD MEHDI SHAH MANSOURI

did knowingly and intentionally conspire and agree to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce certain writings, signs, signals, and sounds in furtherance of such scheme and artifice, contrary to Title 18, United States Code, Section 1343.

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

COUNTS 3 AND 4
(Intentional Damage to a Protected Computer)

1. The allegations contained in paragraphs 1 through 13, 16, and 17 of Count 1 of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. On or about each of the dates set forth below, in the District of New Jersey, and elsewhere, defendants

FARAMARZ SHAHI SAVANDI and
MOHAMMAD MEHDI SHAH MANSOURI

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, and the offense caused loss to persons during a 1-year period from Defendants' course of conduct affecting protected computers aggregating at least $5,000 in value, and caused damage affecting 10 or more protected computers during a 1-year period, described below for each count, each transmission constituting a separate count:

COUNT	DATE	VICTIM
3	January 11, 2016	Mercer County Business in Mercer County, New Jersey
4	April 25, 2017	City of Newark in Newark, New Jersey

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

COUNTS 5 AND 6
(Transmitting a Demand in Relation to Damaging a Protected Computer)

1. The allegations contained in paragraphs 1 through 13, 16, and 17 of Count 1 of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. On or about each of the dates set forth below, in the District of New Jersey, and elsewhere, defendants

FARAMARZ SHAHI SAVANDI and
MOHAMMAD MEHDI SHAH MANSOURI,

with intent to extort from persons money and other things of value, transmitted 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 such damage was caused to facilitate the extortion, described below for each count, each transmission constituting a separate count:

COUNT	DATE	VICTIM
5	January 11, 2016	Mercer County Business in Mercer County, New Jersey
6	April 25, 2017	City of Newark in Newark, New Jersey

In violation of Title 18, United States Code, Sections 1030(a)(7)(C) and (c)(3)(A), and 2.

FORFEITURE ALLEGATION AS TO COUNTS 1, 3, 4, 5, and 6

1. As a result of committing the offenses charged in Counts 1, 3, 4, 5, and 6 of this Indictment, defendants

FARAMARZ SHAHI SAVANDI and
MOHAMMAD MEHDI SHAH MANSOURI

shall forfeit to the United States

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 the offenses charged in Counts 1, 3, 4, 5, and 6 of this Indictment; and

b. pursuant to Title 18, United States Code, Section 1030(i), all right, title, and interest in any personal property that was used or intended to be used to commit or to facilitate the commission of the offenses charged in Counts 1, 3, 4, 5, and 6 of this Indictment.

FORFEITURE ALLEGATION AS TO COUNT 2

2. As a result of committing the offenses charged in Count 2 of this Indictment, defendants

FARAMARZ SHAHI SAVANDI and
MOHAMMAD MEHDI SHAH MANSOURI

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, all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of the said offense, and all property traceable thereto.

SUBSTITUTE ASSETS PROVISION
(Applicable to All Forfeiture Allegations)

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

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 shall be entitled, pursuant to 21 U.S.C. § 853(p) (as incorporated by 28 U.S.C. § 2461(c) and 18 U.S.C. §§ 982(b) and 1030(i)), to forfeiture of any other property of the defendants up to the value of the above-described forfeitable property.

A TRUE BILL:

~~FOREPERSON~~

CRAIG CARPENITO
UNITED STATES ATTORNEY

BRIAN A. BENCZKOWSKI
ASSISTANT ATTORNEY GENERAL

ATTACHMENT A: RANSOM NOTE TO CITY OF NEWARK (REDACTED)

#What happened to your files?

All your files encrypted with RSA-2048 encryption, For more information search in Google "RSA Encryption"

#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need one key for encryption and one key for decryption
So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can get your private key in 3 easy step:

Step1: You must send us 1.7 BitCoin for each affected PC OR 24 BitCoins to receive ALL Private Keys for ALL affected PC's.

Step2: After you send us 1.7 BitCoin, Leave a comment on our Site with this detail: Just write Your "Host name" in your comment

*Your Host name is: [redacted]

Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

*Our Site Address:http:/[redacted]onion/[redacted]

*Our BitCoin Address:[redacted]

(If you send us 24 BitCoins for all PC's, Leave a comment on our site with this detail: Just write "For All Affected PC's" in your comment)
(Also if you want pay for "all affected PC's" You can pay 12 Bitcoins to receive half of keys(randomly) and after you verify it send 2nd half to receive all keys)

How To Access To Our Site

For access to our site you must install Tor browser and enter our site URL in your tor browser.
You can download tor browser from https://www.torproject.org/download/download.html.en
For more information please search in Google "How to access onion sites"

Test Decryption

Check our site, You can upload 2 encrypted files and we will decrypt your files as demo.

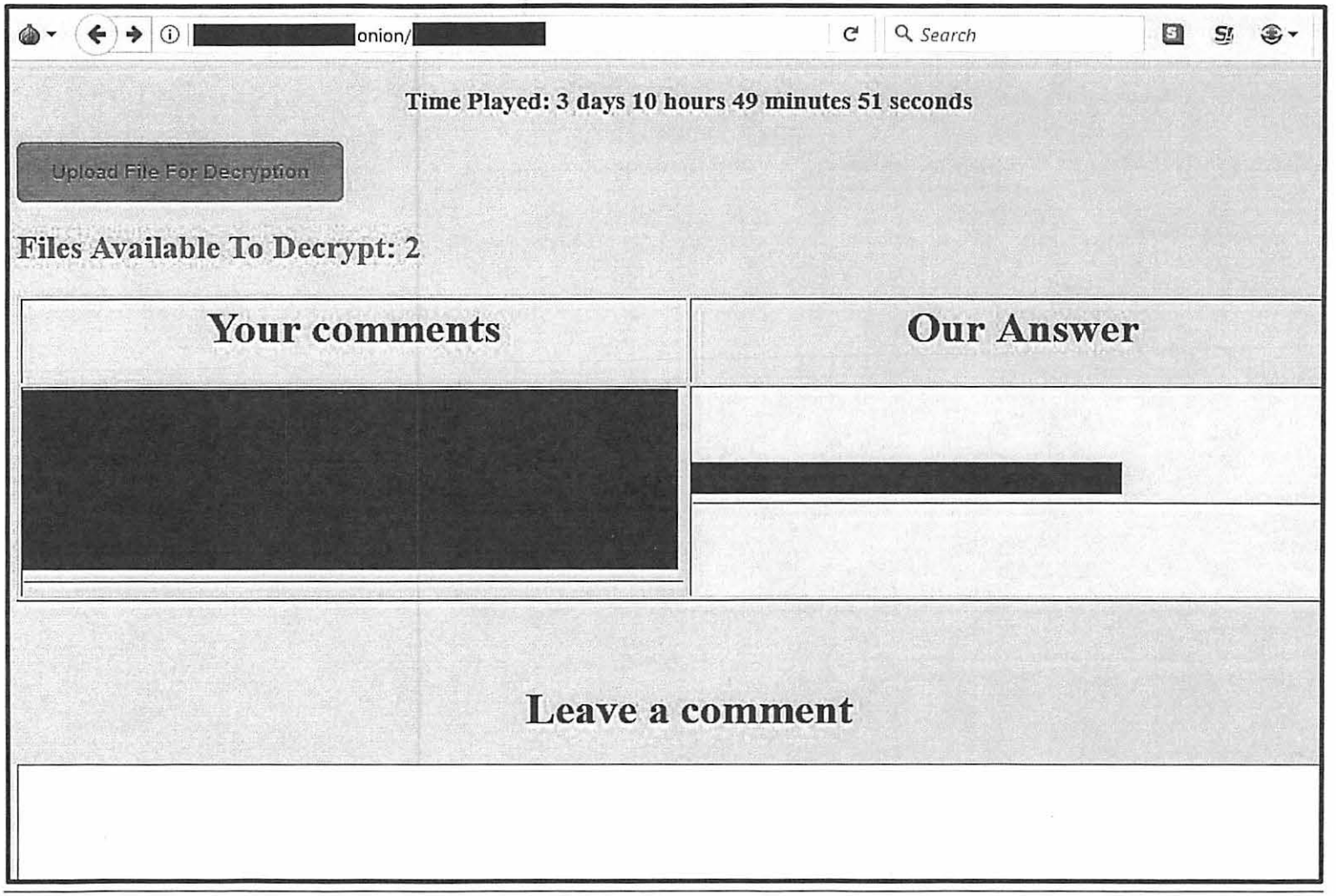
#Where to buy Bitcoin

We advice you to buy Bitcoin with Cash Deposit or WesternUnion From https://localbitcoins.com/ or https://coincafe.com/buybitcoinswestern.php
Because they don't need any verification and send your Bitcoin quickly.

#deadline

You just have 7 days to send us the BitCoin after 7 days we will remove your private keys and it's impossible to recover your files

ATTACHMENT B: RANSOM WEBPAGE FOR CITY OF ATLANTA (REDACTED)



CASE NUMBER: 2016R00103

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

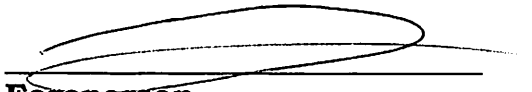
v.

FARAMARZ SHAHI SAVANDI, and
MOHAMMAD MEHDI SHAH MANSOURI

INDICTMENT FOR

18 U.S.C. §§ 371, 1030(a)(5)(A), 1030(a)(7)(C), 1349, and 2

A True Bill,



Foreperson

CRAIG CARPENITO
U.S. ATTORNEY
NEWARK, NEW JERSEY

JUSTIN S. HERRING
ASSISTANT U.S. ATTORNEY
WILLIAM A. HALL
SENIOR COUNSEL

USA-48AD 8
(Ed. 1/97)