U.S. Department of
JUSTICE

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NORTH CAROLINA
EASTERN DIVISION

NO. 4:24-CR-16-M-BM

UNITED STATES OF AMERICA	)	
	)	
v.	)	**INDICTMENT**
	)	
SINA GHOLINEJAD a/k/a "Sina Ghaaf"	)	

The Grand Jury charges:

General Allegations

At all times relevant to the indictment:

1. The defendant, SINA GHOLINEJAD, a/k/a "Sina Ghaaf," was an individual residing overseas, including in Iran.

2. From at least in or about January 2019, and continuing through at least in or about March 2024, GHOLINEJAD and others known and unknown to the Grand Jury were part of a conspiracy to deploy a ransomware variant known as "Robbinhood" to (i) encrypt files on victim computer systems in the United States and elsewhere, (ii) disrupt or negatively impact the victim entities' operations by making files inaccessible, and (iii) block the victims' access to these files until the victims paid a ransom. The conspirators also sometimes stole victim data to pressure victims into paying the ransom.

3. The Robbinhood ransomware also generated ransom notes when deployed. Those ransom notes often directed the victims to pay Bitcoin to specified Bitcoin addresses, or to contact the conspirators using the Robbinhood Ransomware through a Darknet website or email address to obtain the ransom amount.

4. The Robbinhood ransomware caused city governments, corporations, health care organizations, and other entities, in the Eastern District of North Carolina and elsewhere, to suffer tens of millions of dollars of losses. Some of the victim organizations included:

a. the City of Greenville, North Carolina, which was a municipality in the Eastern District of North Carolina;

b. the City of Gresham, Oregon;

c. the City of Baltimore, Maryland;

d. Meridian Medical Group – Specialty Care, P.C., which was an entity in New Jersey;

e. the City of Yonkers, New York;

f. Berkshire Farm Center and Services for Youth, Inc., which was a non-profit organization in New York; and

g. Glenn-Colusa Irrigation District, which was an entity in California.

5. The "Darknet" was a part of the Internet that is encrypted and accessible through the Onion Router (Tor) network, a network of computers on the Internet using specific software and configurations designed to conceal the true IP addresses of the computers on the network. The Tor software allowed a browser to gain access to the Tor network, resolve websites on the Tor network (which use the .onion domain) ("Darknet websites"), and ultimately connect to the computer(s)

hosting the website. Unlike computers on the ordinary internet, which are all assigned a publicly registered IP address and whose location can usually be determined, computers on the Tor network cannot be easily identified or located.

6. "Ransomware" was a type of malicious software or malware that used encryption to block access to a computer, or certain files thereon, until the victim paid a ransom. By blocking access to a computer, or certain files, ransomware was designed to negatively impact the ability of victim entities from functioning normally and forcing them to pay a ransom to regain access to their computers and files.

7. "Virtual currency" or "cryptocurrency" was a digital form of value that was circulated over the Internet and was not backed by a government. Bitcoin (BTC) was one of the most popular forms of virtual currency. Virtual currencies, such as Bitcoin, used a decentralized, peer-to-peer, worldwide consensus network to enable the transfer of value. They may be used as a substitute for fiat currency—such as U.S. dollars—to buy goods or services, or they can be exchanged for fiat or other cryptocurrencies. Payments or transfers of value made with virtual currencies were typically recorded on a distributed public ledger or blockchain that contains an immutable and historical record of every transaction. Although the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. Further, to gain greater anonymity, an individual could set up multiple virtual currency addresses and associated virtual accounts called wallets.

8. A "virtual private server" (VPS) provided computing capability (e.g., to run a website) to a user that is segregated from other users by software restrictions. A single physical server could run multiple VPSs. However, each VPS on a physical server could be used independently with different operating systems and applications. Internet hosting providers could often lease VPS capabilities as a service, but the user controlled the activities and data on the leased VPS.

9. A "virtual private network" (VPN) established a secure connection between users on the internet. A VPN was created by establishing a virtual point to point connection through the use of dedicated circuits or tunneling protocols.

COUNT ONE

10. Paragraphs 1 through 9 are realleged and incorporated herein as though fully set forth in this count.

Object of the Conspiracy

11. From an unknown date, but beginning no later than in or about January 2019, and continuing through at least in or about March 2024, in the Eastern District of North Carolina and elsewhere, the defendant, SINA GHOLINEJAD, a/k/a "Sina Ghaaf," did knowingly conspire, combine, confederate, and agree, with one or more persons, known and unknown to the Grand Jury, to commit offenses against the United States, that is:

a. To intentionally access a computer without authorization, and thereby obtain information from a protected computer, for

purposes of private financial gain, all in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i);

b. 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, thus having caused: (i) loss to one or more persons during a one-year period, and loss resulting from the conspirators' course of conduct affecting one or more protected computers, aggregating at least $5,000; and (ii) damage affecting 10 or more protected computers during a one year period, all in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B); and

c. With intent to extort from any person any money and other thing of value, to 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, all in violation of Title 18, United States Code, Sections 1030(a)(7)(C) and (c)(3)(A).

Manner and Means

12. Members of the conspiracy used the following manner and means, among others, to accomplish the objects of the conspiracy:

a. Leased and maintained VPS accounts at multiple service providers in Europe and elsewhere, including in Bulgaria and the Netherlands. The conspirators used these VPSs to, among other things, host Darknet websites that enabled the conspirators to negotiate ransom demands with victims, operate VPN software to encrypt and anonymize communications, gain and maintain unauthorized access to victim computer networks, and support efforts to transfer the proceeds of victim ransom payments.

b. Registered and operated cryptocurrency wallets for the purposes of financing VPSs and other technologies used in the scheme.

c. Gained and maintained unauthorized access to victim computer networks by using hacking tools and other techniques to exploit vulnerabilities in victim networks and computers. The conspirators also sometimes gained unauthorized access to administrator accounts for victim computer systems and used those accounts to facilitate their ransomware attacks.

d. Copied, transmitted, and stored information and files from the infected victim computers to VPSs controlled by the conspirators from at least around 2022.

e. Deployed the Robbinhood ransomware software on victim computers to encrypt victim computer files and make those files inaccessible to the victims. The Robbinhood Ransomware also saved one or more ransom notes on the victim computers. The encrypted victim files often used the extensions ".enc_robbinhood," ".enc_robbin_hood," or ".rbhd."

f. Extorted victims by requiring the payment of Bitcoin in exchange for the private key required to decrypt the victim computer files. In instances where information and files of the victims were copied and stored by the conspirators, the conspirators also extorted victims by requiring the payment of Bitcoin in exchange for the deletion of that stolen information and files.

g. Received ransom payments in Bitcoin and caused the transfer of the proceeds of these payments in Bitcoin and other cryptocurrencies.

h. Registered and used tools to obfuscate the recipients of the ransom payments, such as cryptocurrency mixing services and chain-hopping (i.e., moving assets between different types of cryptocurrency).

i. Registered, administered and used VPN technologies to encrypt and anonymize their activities, including to obfuscate their identities when logging into VPSs involved in executing the ransomware attacks or cryptocurrency wallets that received ransomware payments.

j. Conducted research using an online search engine to support efforts to hack into victim computer systems, develop and deploy the Robbinhood ransomware, and extort victims.

Overt Acts

13. In furtherance of the conspiracy and to effect the objects thereof, a member of the conspiracy committed at least one of the following overt acts in the Eastern District of North Carolina and elsewhere:

a. On or about March 2, 2019; September 8, 2019; April 15, 2020; March 19, 2021; July 14, 2022; and February 8, 2023, a member of the conspiracy registered VPS infrastructure at a provider in Bulgaria.

b. On or about March 3, 2019, the defendant, SINA GHOLINEJAD, a/k/a "Sina Ghaaf," conducted online research to create the Robbinhood Ransomware ransom note.

c. On or about April 7, 2019, a member of the conspiracy used unauthorized access to deploy the Robbinhood Ransomware on the City of Gresham, Oregon, computer networks.

d. On or about April 7, 2019, the conspirators extorted the City of Gresham, Oregon, by demanding a ransom in exchange for private keys to decrypt the encrypted files.

e. Between on or about April 9, 2019, and on or about April 10, 2019, a member of the conspiracy used unauthorized access to deploy the Robbinhood Ransomware on the City of Greenville, North Carolina, computer networks.

f. On or about April 10, 2019, the conspirators extorted the City of Greenville, North Carolina, by demanding a ransom paid in Bitcoin in exchange for private keys to decrypt the encrypted files.

g. Between on or about May 3, 2019, and on or about May 7, 2019, a member of the conspiracy maintained unauthorized access to the City of Baltimore, Maryland, computer networks.

h. Between on or about May 4, 2019, through on or about May 7, 2019, the defendant, SINA GHOLINEJAD, a/k/a "Sina Ghaaf," conducted online research to further the unauthorized access to the City of Baltimore, Maryland, computer networks.

i. On or about May 7, 2019, a member of the conspiracy used unauthorized access to deploy the Robbinhood Ransomware on the City of Baltimore, Maryland, computer networks.

j. On or about May 7, 2019, the conspirators extorted the City of Baltimore, Maryland, by demanding a ransom paid in Bitcoin in exchange for private keys to decrypt the encrypted files.

k. Between on or about May 12, 2019, and on or about May 25, 2019, the defendant, SINA GHOLINEJAD, a/k/a "Sina Ghaaf," conducted online research to facilitate the extortion of the City of Baltimore, Maryland.

l. Between on or about May 12, 2019, and on or about June 3, 2019, the conspirators further extorted the City of Baltimore, Maryland, by posting information publicly using the Twitter account @robihkjn.

m. On or about July 19, 2019; November 8, 2019; July 15, 2021; and February 11, 2022, a member of the conspiracy registered VPS infrastructure at a provider in the Netherlands.

n. On or about October 14, 2020, a member of the conspiracy used unauthorized access to deploy the Robbinhood Ransomware on the Meridian Medical Group – Specialty Care, P.C., computer networks.

o. On or about October 14, 2020, the conspirators extorted Meridian Medical Group – Specialty Care, P.C., by demanding a ransom paid in Bitcoin in exchange for private keys to decrypt the encrypted files.

p. On or about September 6, 2021, a member of the conspiracy used unauthorized access to deploy the Robbinhood Ransomware on the City of Yonkers, New York, computer networks.

q. On or about September 6, 2021, the conspirators extorted the City of Yonkers, New York, by demanding a ransom paid in Bitcoin in exchange for private keys to decrypt the encrypted files.

r. On or about July 19, 2022, a member of the conspiracy used unauthorized access to deploy the Robbinhood Ransomware on the Berkshire Farm Center and Services for Youth, Inc., computer networks.

s. On or about July 19, 2022, the conspirators extorted the Berkshire Farm Center and Services for Youth, Inc., by demanding a ransom paid in Bitcoin in exchange for private keys to decrypt the encrypted files.

t. On or about June 5, 2023, a member of the conspiracy used unauthorized access to deploy the Robbinhood Ransomware on the Glenn-Colusa Irrigation District computer networks.

u. On or about June 5, 2023, the conspirators extorted the Glenn-Colusa Irrigation District by demanding a ransom in exchange for private keys to decrypt the encrypted files.

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

COUNT TWO

14. Paragraphs 1 through 9 are realleged and incorporated herein as though fully set forth in this count.

15. From an unknown date, but beginning no later than on or about April 9, 2019, and continuing until on or about April 10, 2019, in the Eastern District of North Carolina and elsewhere, the defendant, SINA GHOLINEJAD, a/k/a "Sina Ghaaf," and others known and unknown to the Grand Jury knowingly caused the transmission of a program, information, code, and command, and aided and abetted the same, and, as the result of such conduct, intentionally caused damage without authorization to protected computers, that is, computers for the City of Greenville, North Carolina, and the offense caused (a) loss to one or more persons during a one-year period, and loss resulting from a related course of conduct affecting one or more protected computers, aggregating at least $5,000; and (b) damage affecting 10 or more protected computers during a one-year period.

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

COUNT THREE

16. Paragraphs 1 through 9 are realleged and incorporated herein as though fully set forth in this count.

17. From an unknown date, but beginning no later than on or about April 9, 2019, and continuing until on or about April 10, 2019, in the Eastern District of North Carolina and elsewhere, the defendant, SINA GHOLINEJAD, a/k/a "Sina

Ghaaf," and others known and unknown to the Grand Jury, with the 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, that is, computers for the City of Greenville, North Carolina, and aided and abetted the same, where such damage was caused to facilitate the extortion.

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

COUNT FOUR

18. Paragraphs 1 through 9 are realleged and incorporated herein as though fully set forth in this count.

19. From an unknown date, but beginning no later than on or about May 3, 2019, and continuing until at least on or about June 3, 2019, the defendant SINA GHOLINEJAD, a/k/a "Sina Ghaaf," who will first be brought to the Eastern District of North Carolina within the meaning of 18 U.S.C. § 3238, and others known and unknown to the Grand Jury, knowingly caused the transmission of a program, information, code, and command, and aided and abetted the same, and, as the result of such conduct, intentionally caused damage without authorization to protected computers, that is, computers for the City of Baltimore, Maryland, and the offense caused (a) loss to one or more persons during a one-year period, and loss resulting from a related course of conduct affecting one or more protected computers,

aggregating at least $5,000; and (b) damage affecting 10 or more protected computers during a one-year period.

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

COUNT FIVE

20. Paragraphs 1 through 9 are realleged and incorporated herein as though fully set forth in this count.

21. From an unknown date, but beginning no later than on or about May 3, 2019, and continuing until at least on or about June 3, 2019, the defendant SINA GHOLINEJAD, a/k/a "Sina Ghaaf," who will first be brought to the Eastern District of North Carolina within the meaning of 18 U.S.C. § 3238, and others known and unknown to the Grand Jury, with the 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, that is, computers for the City of Baltimore, Maryland, and aided and abetted the same, where such damage was caused to facilitate the extortion.

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

COUNT SIX

22. Paragraphs 1 through 9 and 12 are realleged and incorporated herein as though fully set forth in this count.

23. From an unknown date, but beginning no later than in or about January 2019, and continuing through at least in or about March 2024, in the Eastern District of North Carolina and elsewhere, the defendant, SINA GHOLINEJAD, a/k/a "Sina Ghaaf," did knowingly and willfully combine, conspire, confederate, and agree, with one or more persons, both known and unknown to the Grand Jury, to commit an offense against the United States, that is, to knowingly devise and intend to devise a scheme and artifice to defraud and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, for which one or more conspirators transmitted and caused to be transmitted by means of wire communications in interstate and foreign commerce certain writings, signs, signals, pictures, and sounds, for the purpose of executing the scheme and artifice, in violation of Title 18, United States Code, Section 1343.

All in violation of Title 18, United States Code, Section 1349.

COUNT SEVEN

24. Paragraphs 1 through 9 and 12 are realleged and incorporated herein as though fully set forth in this count.

25. From an unknown date, but beginning no later than in or about January 2019, and continuing through at least in or about March 2024, in the Eastern District of North Carolina and elsewhere, the defendant, SINA GHOLINEJAD, a/k/a "Sina Ghaaf," did knowingly conspire, combine, confederate, and agree with other individuals, both known and unknown to the Grand Jury, to commit offenses against the United States, that is, to knowingly conduct and attempt to conduct financial

transactions affecting interstate commerce and foreign commerce, which transactions involved the proceeds of a specified unlawful activity, that is, Computer Fraud, in violation of 18 U.S.C. § 1030, knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of such specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

All in violation of Title 18, United States Code, Section 1956(h).

(Remainder of page intentionally left blank.)

FORFEITURE

Notice is hereby given that all right, title and interest in the property described herein is subject to forfeiture.

Upon conviction of any offense charged herein constituting "specified unlawful activity" (as defined in 18 U.S.C. §§ 1956(c)(7) and 1961(1)), or a conspiracy to commit such offense, the defendant shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C), as made applicable by 28 U.S.C. § 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the said offense.

Upon conviction of any felony violation of the monetary transaction offenses charged herein (including any violation of 18 U.S.C. § 1956), the defendant shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(1), any property, real or personal, involved in such offense, and any property traceable to such property.

Upon conviction of any violation of, or conspiracy to violate, Section 1030 of Title 18 of the United States Code, the defendant shall forfeit to the United States, pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i)(1)(B), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of the said offense, or, pursuant to 18 U.S.C. § 1030(i)(1)(A), any personal property that was used or intended to be used to commit or to facilitate the commission of the said offense.

If any of the above-described forfeitable property, as a result of any act or omission of a defendant: cannot be located upon the exercise of due diligence; has been transferred or sold to, or deposited with, a third party; has been placed beyond the jurisdiction of the court; has been substantially diminished in value; or has been

commingled with other property which cannot be divided without difficulty; it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of said defendant up to the value of the forfeitable property described above.

REDACTED VERSION
Pursuant to the E-Government Act and the federal rules, the unredacted version of this document has been filed under seal.

04/03/2024
DATE

MICHAEL F. EASLEY, JR.
United States Attorney

BY: BRADFORD M. DEVOE
Assistant United States Attorney

AARASH HAGHIGHAT
RYAN K.J. DICKEY
Senior Counsels
Criminal Division, Computer Crime and Intellectual Property Section