UNITED STATES DISTRICT COURT

for the

District of Colorado

United States of America)
v.)
)
ISAAC RAFAEL JORGE ROMERO)
and)
JOSE ALEJANDRO OSORIO ECHEGARAY)

Case No. 17-mj-20-gpg

17-mj-116-RMS

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief:

On or about the date(s) of 10 October 2017, in the county of Douglas in the State and District of Colorado, the defendant (s) violated:

Code Section	*Offense Description*
18 U.S.C. Section 1030(a)(4)	Fraud and related activity in connection with computers
18 U.S.C. Section 2113(b)	Bank robbery and incidental crimes

This criminal complaint is based on these facts:

See Affidavit attached hereto and herein incorporated by reference.

X Continued on attached sheet.

s/Jeffrey W. Holmes
Complainant's signature

Jeffrey W. Holmes, Special Agent - FBI
Printed name and title

Sworn to before me and: ☐ signed in my presence.
☒ submitted, attested to, and acknowledged by reliable electronic means.

Date: 11/17/2017

Judge's signature

City and state: Grand Junction, CO

Gordon P. Gallagher, USMJ
Printed name and title

DEFENDANT: ISAAC RAFAEL JORGE ROMERO

YOB: 1988

ADDRESS (CITY/STATE): 3030 Greenridge Dr, Apt 69, Houston, TX 77057

OFFENSE(S): 18 U.S.C. Section 1030(a)(4), Fraud and related activity in connection with computers;
18 U.S.C. Section 2113(b), Bank robbery and incidental crimes

LOCATION OF OFFENSE (COUNTY/STATE): Douglas, CO;

PENALTY: 18 U.S.C. Section 1030(a)(4) – NMT 5 years, NMT $250,000 fine, or both; NMT 3 years supervised release; $100 special assessment.
18 U.S.C. Section 2113(b) – NMT 10 years, NMT $250,000 fine, or both; NMT 3 years supervised release; $100 special assessment.

AGENT: Jeffrey W. Holmes
Special Agent, Federal Bureau of Investigation

AUTHORIZED BY: Andrea Surratt
Assistant U.S. Attorney

ESTIMATED TIME OF TRIAL:

__x__ five days or less _____ over five days _____ other

THE GOVERNMENT

___X__ will seek detention in this case based on 18 U.S.C. § 3142(f)([**1** or 2])

_____will not seek detention

The statutory presumption of detention **is not** applicable to this defendant.

OCDETF CASE: _____ Yes __x___ No

DEFENDANT: JOSE ALEJANDRO OSORIO ECHEGARAY

YOB: 1987

ADDRESS (CITY/STATE): Unknown

OFFENSE(S): 18 U.S.C. Section 1030(4), Fraud and related activity in connection with computers;
18 U.S.C. Section 2113(b), Bank robbery and incidental crimes

LOCATION OF OFFENSE (COUNTY/STATE): Douglas, CO;

PENALTY: 18 U.S.C. Section 1030(a)(4) – NMT 5 years, NMT $250,000 fine, or both; NMT 3 years supervised release; $100 special assessment.
18 U.S.C. Section 2113(b) – NMT 10 years, NMT $250,000 fine, or both; NMT 3 years supervised release; $100 special assessment.

AGENT: Jeffrey W. Holmes
Special Agent, Federal Bureau of Investigation

AUTHORIZED BY: Andrea Surratt
Assistant U.S. Attorney

ESTIMATED TIME OF TRIAL:

__x__ five days or less _____ over five days _____ other

THE GOVERNMENT

___X__ will seek detention in this case based on 18 U.S.C. § 3142(f)([**1** or 2])

_____will not seek detention

The statutory presumption of detention **is not** applicable to this defendant.

OCDETF CASE: _____ Yes __x__ No

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

1. Your affiant, Jeffrey W. Holmes, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn depose and state as follows to wit:

2. Your affiant has been employed by the FBI for 10 years. Prior to my FBI employment, I received a Bachelor's of Science degree in Computer Science and worked for several years as a computer programmer and network and systems administrator. As part of my duties, I investigate criminal violations relating to computer intrusions in violation of Title 18, United States Code, Section 1030 and other computer related crimes. I have received training and instruction in the field of investigations of computer intrusions and other computer related crimes and have had the opportunity to participate in investigations relating to computer intrusions and fraudulent activity. Additionally, I have received training and am certified to process and examine digital evidence.

3. The facts in support of this affidavit and contained in the following paragraphs are the result of an investigation to identify the subject(s) who used malicious software ("malware") to conduct thefts from Automated Teller Machines (ATMs).

4. This affidavit is being submitted in support of a criminal complaint and affidavit charging Isaac Rafael Jorge Romero and Jose Alejandro Osorio Echegaray with violation of Title 18, United States Code, Section 1030(a)(4), fraud and related activity in connection with computers and Title 18, United States Code 2113(b), bank robbery and incidental crimes. Due to the limited purpose of this affidavit, your affiant has not included each and every fact known concerning this investigation, although, to the best of his information, knowledge and belief, your affiant has not omitted any material fact that undermines the statements and conclusions herein. Your affiant has set forth only the facts your affiant believes are necessary to establish probable cause to show that Isaac Rafael Jorge Romero and Jose Alejandro Osorio Echegaray committed fraud by unauthorized access to a protected computer and bank robbery and incidental crimes, in violation of Title 18, United States Code, Section 1030(a)(4) and Title 18, United States Code 2113(b).

RELEVANT STATUTES

5. This investigation concerns alleged violations of 18 U.S.C. Section 1030(a)(4), relating to knowingly and with intent to defraud, accesses a protected computer without authorization, and by means of such conduct further the intended fraud and obtains anything of value and 18 U.S.C. Section 2113(b), relating to stealing money in possession of a bank, credit union, or savings and loan association.

6. 18 U.S.C. Section 1030(a)(4) prohibits a person from knowingly and with intent to defraud, access a protected computer without authorization, or exceed authorized access, and by means of such conduct further the intended fraud and obtain anything of value. Pursuant to Section 1030(e)(2)(A), a "protected computer" includes a computer exclusively for the use of a financial institution.

7. 18 U.S.C. Section 2113(b), prohibits a person, with the intent to steal or purloin, from taking or carrying away, any property or money or other thing of value exceeding $1,000 belonging to, or in the care, custody, control, management, or possession of any bank, credit union, or any savings and loan association.

INVESTIGATION

8. This investigation was initiated when Public Service Credit Union (PSCU) reported a theft from one of their ATMs located in Parker, Colorado. The accounts of PSCU are insured by the National Credit Union Administration Board.

9. On 10 October 2017 at approximately 9:18PM, two white males entered the vestibule area of the PSCU, Parker, Colorado branch, located at 11061 South Parker Road, Parker, Colorado 80134. Although the branch was closed at the time, the vestibule area remained open to allow customers to access the ATM located there. Surveillance video shows the two subjects approach the ATM and open the "top hat" section of the ATM. This section contains the computer and associated hard drive for the ATM but not the secured vault where the cash is stored. The subjects can be seen on surveillance video reaching into the ATM, and then closing it and exiting the vestibule. On the video, one of the subjects appears to be carrying an object consistent with the size and appearance of the hard drive from ATM.

10. Approximately ten minutes later, the subjects returned to the vestibule area. Based on the surveillance video, one of the subjects appears to be holding something inside the front pocket of his hooded sweatshirt. The subjects opened the ATM top hat area of the ATM again and appear to be working inside of it. They then closed the top hat and appear to wait while the ATM computer starts. After the ATM restarted, both subjects can be seen on the video using their mobile phones. One of the subjects appeared to be holding a small wireless mini-computer keyboard. The subjects then began retrieving cash from the ATM dispenser. At one point one of the subjects can be seen receiving a backpack outside the vestibule area from an unidentifiable third subject. The two subjects appeared to use the backpack to hold the cash dispensed from the ATM.

11. At approximately 9:50PM the subjects opened the top hat of the ATM again. The subjects then closed the top hat and exited the vestibule.

12. A subsequent audit of the ATM by PSCU determined that $24,000 was missing from the ATM. Examination of the ATM determined that the hard drive cover, inside the top hat section, had been pried open. Forensic analysis of the ATM hard drive determined that during the time the two subjects were seen accessing the ATM, malicious software ("malware") was installed on the ATM hard drive. The malware is known as PLOUTOS-D, also known as PLOUTUS-D, and allows an attacker to subvert the normal ATM process and dispense cash without accounting or authorization from the bank. This attack is known as "jackpotting." Often the malware requires entering of codes to dispense the cash. These codes can be obtained by a third party, not at the location, who then provides the codes to the subjects at the ATM. This allows the third party to know how much cash is dispensed from the ATM, preventing those who are physically at the ATM from keeping cash for themselves instead of providing it to the criminal organization. Use of mobile phones is often used to obtain these dispensing codes.

13. In November 2017, similar ATM thefts were uncovered in the Saint George, Utah area. Surveillance images from one of the ATMs appeared to show the same subjects that were at the PSCU Parker, Colorado PSCU branch. Additional surveillance images identified license plate numbers associated with two vehicles used by other subjects of the ATM thefts in Utah. Investigation determined that the vehicles were rented by Venezuelan nationals. In addition to the two vehicles identified in the surveillance images, the rental car company provided information on a third vehicle, which was rented by Jose Alejandro Osorio Echegaray. Photographs were obtained of Echegaray and he appears to be one of the subjects who physically accessed the PSCU ATM on 10 October 2017.

14. On or about 16 November 2017, Isaac Rafael Jorge Romero, Jose Alejandro Osorio Echegaray, and two other individuals, were arrested in Teton County, Wyoming on controlled substances offenses. I have reviewed booking photographs for both of these defendants, and it appears to me they are the same individuals who participated in the theft of money from the Parker, Colorado PSCU ATM on 10 October 2017. For instance, Romero has a distinctive neck tattoo which is visible on the ATM surveillance and his Teton County booking photograph.

15. Two other subjects of the Utah theft were arrested in San Diego, California when they attempted to return a rental car associated with the theft. After their arrests, these subjects were shown an ATM surveillance photo which was believed to be of Romero. The subjects indicated that Romero was part of the theft but they only knew him as "Isaac." It is believed that the two subjects who physically accessed the PSCU ATM were Venezuelan nationals, Isaac Rafael Jorge Romero, date of birth 2 February 1988, and Jose Alejandro Osorio Echegaray, date of birth 22 April 1981.

16. Public Service Credit Union provided a copy of their National Credit Union Administration (NCUA) certificate. The certificate number is 64778, dated 15 December 1978 and indicates PSCU is a federally insured credit union.

###

17. Based on the above captioned information, it is requested that a warrants be issued for Isaac Rafael Jorge Romero, and Jose Alejandro Osorio Echegaray, for fraud by unauthorized access to a protected computer and bank robbery and incidental crimes, in violations of Title 18, United States Code, Section 1030(a)(4) and Title 18, United States Code 2113(b).

s/Jeffrey W. Holmes
Jeffrey W. Holmes, Special Agent
FBI

Subscribed and sworn to before me this 17th day of November 2017.

U.S. MAGISTRATE JUDGE
Gordon P. Gallagher

Affidavit reviewed and submitted by Andrea Surratt, Assistant United States Attorney.

AO 442 (Rev. 11/11) Arrest Warrant

UNITED STATES DISTRICT COURT

for the

District of Colorado

United States of America
v.

ISAAC RAFAEL JORGE ROMERO

Defendant

Case No. 17-mj-20-gpg

ARREST WARRANT

TO: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay *(name of person to be arrested)* ISAAC RAFAEL JORGE ROMERO, who are accused of an offense or violation based on the following document filed with the court:

☐Indictment ☐Superseding Indictment ☐Information ☐Superseding Information ☒Complaint

☐Probation Violation Petition ☐Supervised Release Violation Petition ☐Violation Notice ☐Order of the Court

This offense is briefly described as follows:

18 U.S.C. Section 1030(a)(4) (fraud and related activity in connection with computers)

AND

18 U.S.C. Section 2113(b) (bank robbery and incidental crimes)

Date: 11/17/2017

Issuing officer's signature

City and state: Grand Junction, CO

Gordon P. Gallagher, USMJ
Printed name and title

Return

This warrant was received on *(date)* _____, and the person was arrested on *(date)* _____

at *(city and state)* _____.

Date: _____

Arresting officer's signature

Printed name and title

UNITED STATES DISTRICT COURT

AO 442 (Rev. 11/11) Arrest Warrant

for the

District of Colorado

United States of America
v.

JOSE ALEJANDRO OSORIO ECHEGARAY

Defendant

Case No. 17-mj-20-gpg

ARREST WARRANT

TO: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay *(name of person to be arrested)* JOSE ALEJANDRO OSORIO ECHEGARAY, who are accused of an offense or violation based on the following document filed with the court:

☐Indictment ☐Superseding Indictment ☐Information ☐Superseding Information ☒Complaint

☐Probation Violation Petition ☐Supervised Release Violation Petition ☐Violation Notice ☐Order of the Court

This offense is briefly described as follows:

18 U.S.C. Section 1030(a)(4) (fraud and related activity in connection with computers)

AND

18 U.S.C. Section 2113(b) (bank robbery and incidental crimes)

Date: 11/17/2017

Issuing officer's signature

City and state: Grand Junction, CO

Gordon P. Gallagher, USMJ

Printed name and title

Return

This warrant was received on *(date)* _____, and the person was arrested on *(date)* _____ at *(city and state)* _____.

Date: _____

Arresting officer's signature

Printed name and title