

U.S. DISTRICT COURT
DISTRICT OF VERMONT
FILED

UNITED STATES DISTRICT COURT

for the

District of Vermont

2017 APR 21 PM 4:46

CLERK

BY LAW
DEPUTY CLERKUnited States of America
v.

JOSIAH LEACH

Case No.

2:17mj-44-1

Defendant(s)

CRIMINAL COMPLAINT

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

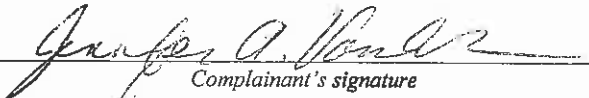
On or about the date(s) of April 18, 2017 through April 21, 2017 in the county of Chittenden in the
 District of Vermont , the defendant(s) violated:*Code Section*

18 U.S.C. § 875(c)

*Offense Description*Knowingly transmitting in interstate commerce a communication containing a
threat to injure the person of another.

This criminal complaint is based on these facts:

See attached Affidavit.

☒ Continued on the attached sheet.
Complainant's signature

Jennifer Vander Veer, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 4/21/17
Judge's signatureCity and state: Burlington, Vermont

Hon. Christina Reiss, Chief U.S. District Court Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF VERMONT

AFFIDAVIT

I, Jennifer A. Vander Veer, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of charging JOSIAH LEACH with knowingly transmitting in interstate commerce communications containing threats to injure the person of another on or about April 18-21, 2017, in violation of 18 U.S.C. §875(c).

2. I am a Special Agent with the United States Federal Bureau of Investigation (FBI), and have been since 2008. I am assigned to the cyber squad of the FBI's Albany Field Office where I am responsible for investigating high-tech crimes, including cyber-based terrorism, espionage, computer intrusions, and major cyber fraud. Prior to joining the FBI, I held the position of Internet Operations Manager at a private company in Vermont for eight years, and also worked as a Software Development Intern for a large technology company in California.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested charge and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that from in or about April 18, 2017 through in or about April 21, 2017, JOSIAH LEACH violated 18 U.S.C. 875(c) (Interstate threats to injure another person)

by transmitting threats indicating his intention to kill and harm students and faculty at South Burlington High School.

INCIDENT SUMMARY

5. As explained in more detail below, between 4/18/2017 and 4/21/2017 certain students and teachers South Burlington High School (SBHS) received multiple emails threatening physical harm to students and faculty members. I have reviewed these emails. I also learned that during this time an employee at SBHS received a phone call during which the caller threatened to kill persons at SBHS. During the same time period, South Burlington Police Department (SBPD) received a similar, apparently related threat via Facebook message. The threats led to school lockdowns on April 18, 19, and 20 and cancellation of school on 4/21/2017.

6. I responded to assist the SBPD in the investigation of the threats and have reviewed the information described below between 4/19/2017 and today.

THREAT #1

7. On April 18, 2017, between 11:09:04 to 11:27:29 EDT six emails sent by email account subedimukesh@outlook.com were received by six separate addresses within the South Burlington schools (all receiving accounts ended in sbschools.net). I have reviewed these emails which said, with one slight variation, "I'm going to kill you and all your students soon at south Burlington high school in Vermont. I'm coming for you. Good luck to you all. I'm coming today and if not today, I'll kill you all tomorrow. Take it as a joke or message either way it's fate." [sic]. The South Burlington schools were placed in a state of heightened security following receipt of the messages.

8. I reviewed information received from Microsoft Corporation which operates the

outlook.com email service related to the sending address. Microsoft records indicated that the subedimukesh@outlook.com address was accessed on 4/18/2017 at 11:05:20 Eastern Daylight Time (EDT) from Internet Protocol (IP) address 104.200.140.118. Information from Hosting Services Inc. an internet service provider, stated that IP address 104.200.140.118 resolves to the Virtual Private Network (VPN)¹ service provider betternet.co.

9. Seven screen capture images provided to me by South Burlington High School IT staff showed copies of deleted draft messages in Josiah Leach's South Burlington High School Google Apps account created on 4/18/2017 between 11:21:57 and 11:29:15. Four of the seven draft messages were addressed to recipients of the Threat #1 emails and were created within 30 to 60 seconds of when the threat emails were sent. South Burlington High School IT staff explained that the Google Apps account could be used to look up school network email addresses.

THREAT #2

10. Shortly after the initial threats were received, on April 18, 2017 at approximately 11:45 AM EDT, the SBPD's Facebook account received a message from a Facebook account ending in 9596 stating, "First I am killing everyone at south Burlington high school right now. Then your next. [sic]"

11. Facebook provided records related to the Facebook account ending in 9596 which I reviewed. Those records indicated that the registered name on the account was Mukesh

¹ A VPN is a method of providing encryption to provide secure access to a computer over the internet.

Mukesh, and the account was first registered on 4/18/2017 at 11:35:11 EDT. The records further indicated that all access to this account was from IP address 104.200.140.118, the same IP Address associated with the access to the sending email account involved in Threat #1. Facebook records also provided email addresses jimmymukie98@outlook.com and sjsjsjsis@gmail.com as associated with the account.

12. Microsoft Corporation provided information related to the jimmymukie98@outlook.com address which I reviewed. According to the records, the account was created on 4/18/2017 at 11:37:20 EDT and was accessed from IP address 64.30.37.252 on 4/18/2017 at 11:37:17 EDT. I confirmed that IP Address 64.30.37.252 resolves to the South Burlington School District (sbschools.net), indicating that the person registering and accessing the email account was using the South Burlington School District's servers.

13. Law enforcement reviewed the South Burlington school server logs with permission from the school for activity during this time period. Approximately three students, including Josiah Leach², were identified as connecting to websites associated with Microsoft Outlook within the two minute window on 4/18/2017 when the jimmymukie98@outlook.com email account was created.

14. I conducted further review of network logs and determined that Josiah Leach was conducting this activity from a device with MAC Address³ 10:4A:7D:50:97:09, an Intel laptop.

² Josiah Leach is 18 years old.

³ A MAC address, or media access control address, also called physical address, is a unique identifier assigned to network interfaces for communications on the physical network segment.

This device also had the name: HS-11-G2CHJ52.SBSCHOOLS.NET. South Burlington High School IT staff stated that this was a student laptop owned by the school.

THREAT #3

15. On April 18, 2017 from 14:16:17 to 14:16:53 EDT, the South Burlington High School secretary received a phone call from telephone number 802-472-1939 in which the caller stated in what the secretary described as a raspy voice, “everyone is going to die tomorrow.” I have spoken with law enforcement officers who interviewed the school secretary regarding this call.

16. I have spoken with law enforcement officers who received information from South Burlington High School telephone service provider Sovernet. Sovernet provided them with information that determined that phone number 802-472-1939 was serviced by TextNow.

17. I reviewed records provided by TextNow, a Voice Over Internet Protocol (VOIP)⁴ provider, which indicated that their account for phone number 802-472-1939 was created on April 18, 2017 at 10:16:02 EDT using email address snsjsajab@gmail.com.⁵ Further, TextNow indicated that IP Address 73.114.21.114 was associated with the phone call. Publicly available web resources indicate that IP Address 73.114.21.114 resolves to Comcast Xfinity Wifi.

18. Law enforcement reviewed records from the South Burlington High School computer network which indicated that a device with MAC address D0:5B:A8:FF:E4:5C had

⁴ VOIP is a form of technology that allows the transmission of speech over the internet.

⁵ Records from Google, the provider of gmail, which I reviewed, indicate that this is an invalid email address.

accessed TextNow via the school's servers using Josiah Leach's login credentials (leachj) at 10:15:11 EDT on April 18, 2017.

19. Law enforcement also reviewed records from the South Burlington High School computer network which indicated that the MAC address D0:5B:A8:FF:E4:5C is associated with an with an Andriod Z812 device. Public source research indicate this is a ZTE Maven cell phone. According to records from the South Burlington High School computer network, this device was connected to SBHS networks on 4/18/2017 from 9:59:07 to 11:52:42 EDT.

THREAT #4

20. On April 19, 2017, between 10:51:57 to 10:56:09 EDT, five emails from sender address rustyslack@outlook.com were received by accounts on the South Burlington network. The messages, which I reviewed, stated, "Wow, you guys really thought it was a threat. That's what I wanted you guys to think. Should've taken it seriously. I don't care for my life and don't care for yours. I'm choosing 5 students in my interest to kill today then I'm killing every teacher who gets this mail. We are armed with knives and guns. We know all exits and side doors and windows. We are coming before 1:00pm today. We wasn't joking. Essex only got lucky. GET READY FOR THEORY MURDER. The slacks are coming.."

21. I reviewed records from Microsoft regarding the rustyslack@outlook.com email account which indicated that the account was created on 4/19/2017 at 10:18:34 EDT and was accessed on 4/19/2017 at 10:18:29 and 11:34:06 EDT from IP address 172.98.87.72.

22. Public source information which I reviewed indicated that IP address 172.98.87.72 resolved to Total Server Solutions, who also was the listed registrant for the IP address in Threat #1 which provided service to Betternet.co.

THREAT #5

23. On 4/20/2017 from 11:29:45 to 11:41:48 EDT email address

sbhsmurder2017@outlook.com sent three emails to accounts on the South Burlington school network which stated:

My other threat was only a test. I stood across the Street and saw you evacuating, great job. Now I got to see what students I can kill. I've already hacked into your students emails and servers to see who. You all can keep thinking it's a "low risk". I can already be inside your building right now. I have access to all students and teacher information, check out the murder list. I'm watching you all.

The message then included a "SBHS MURDER LIST" which included the names of five teachers, including reference to one of their locations in the building and eleven students including Josiah Leach. The message concluded:

THIS COULD'VE BEEN PREVENTED FROM KEEPING THE REBEL NAME. NOW I'm gonna have to attack you all, I don't care for my own life as long as you're all dead!!!!

Sincerely,

Unknown.

24. I reviewed information from Microsoft Corporation regarding the sbhsmurder2017@outlook.com account which indicated that the account was accessed on 4/20/2017 at 11:12:19 EDT from IP address 71.161.92.56. Publicly available records indicate that 73.161.92.56 resolved to Fairpoint Communications Inc.

25. I have spoken with law enforcement officers who received information from Fairpoint Communications Inc. Fairpoint Communications Inc. stated that at the time in question, the IP address 71.161.92.56 resolved to JOSIAH LEACH's home address. The account

had been active since August 2016 and was registered under the name Leon McKenzie, who law enforcement officers confirmed was the brother of Josiah Leach.

THREAT #6

26. On 4/20/2017 from 11:47:43 to 11:48:52 EDT email address jimcollins9797@outlook.com sent messages to three email accounts on the South Burlington School network which were identical to the messages received in Threat #5.

27. I reviewed information from Microsoft Corporation regarding the jimcollins9797@outlook.com account which indicated that the account was accessed on 4/20/2017 at 11:45:49 from IP Address 73.114.21.93. Publicly available records indicate that 73.114.21.93 resolved to Comcast Xfinity WIFI.

THREAT #7

28. On 4/21/2017 at 00:57:00 EDT a video was shared on Facebook by Facebook account taylor.isabelle.5496 which appeared to show a young male face which was blurred and voice was altered. The male discussed the threats, stated he was pleased they were taken seriously, and showed an image of the email from threats #5 and 6.

29. Facebook provided records, which I reviewed, indicating that Facebook account taylor.isabelle.5496 was associated with a user in Plattsburgh, New York and has communicated with the Facebook account of Josiah Leach on 4/19/2017 at 22:11 EDT.

THREAT #8

30. On 4/21/2017 at 2:25 EDT an email which I reviewed was sent to nine accounts on the South Burlington High School network from theycallmejim98@gmail.com. The email

contained a video which was law enforcement officers confirmed was identical to the video posted on Facebook in Threat #7.

31. Information provided by Google, Inc. which I have reviewed showed that the email account theycallmejim98@gmail.com was created on 4/21/2017 at 01:08:52 EDT from IP address 71.161.92.56.

32. IP address 71.161.92.56 is the same Fairpoint Communications Inc. address that was associated with the PREMISES in Threat #5.

SUMMARY

33. I conducted a review of South Burlington High School network logs between 4/18/2017 and 4/20/2017. The logs showed that Josiah Leach accessed the network using three unique devices identified by the following MAC addresses and device description:

- a. a ZTE Maven cell, MAC Address: D0:5B:A8:FF:E4:5C;
- b. Intel PC, MAC Address: 10:4A:7D:50:97:09; and
- c. a Samsung SGHI317, MAC Address: 88:32:9B:12:A6:E8.

34. Two of these devices were described conducting activity above. Open source information indicated the third device was a Galaxy Note II cell phone. This device was seen being used on school networks by Josiah Leach during the period of the threats and could have been used to conduct the described activity since not all of the Threats could be attributed to devices due to the use of a VPN and other deceptive tactics.

35. I am aware from my training and experience that the email communications and telephone communications described above traveled by wires in interstate commerce.

CONCLUSION

36. Based on the information outlined above, there is probable cause to believe that from in or about April 18, 2017, through in or about April 21, 2017, JOSIAH LEACH knowingly transmitted in interstate commerce communications containing threats to injure the persons of students and faculty members at the school.

Respectfully submitted,



JENNIFER VANDER VEER
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on April 21, 2017:



CHRISTINA REISS
CHIEF UNITED STATES DISTRICT COURT JUDGE