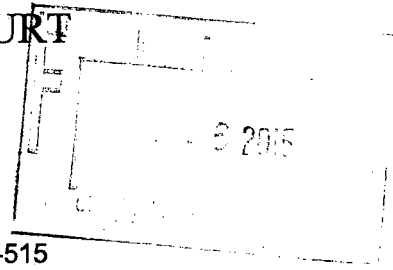


UNITED STATES DISTRICT COURT

for the Eastern District of Virginia



United States of America v. ARDIT FERIZI a/k/a Th3Dir3ctorY,

Case No. 1:15-MJ-515

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) 4/01/15 to or on about 8/11/15 in the extraterritorial jurisdiction of U.S. and in the Eastern District of Virginia, the defendant(s) violated:

Table with 2 columns: Code Section, Offense Description. Rows include 18 U.S.C. § 1030, 1028A, 2339B and offenses like Unauthorized access to a computer, Aggravated identity theft, and Providing material support to a designated foreign terrorist group.

This criminal complaint is based on these facts: See attached affidavit.

Continued on the attached sheet.

Reviewed by AUSA/SAUSA:

AUSA Lynn E. Haaland

Handwritten signature of Kevin M. Gallagher

Complainant's signature

Special Agent Kevin M. Gallagher

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/06/2015

Handwritten signature of Theresa Carroll Buchanan

Theresa Carroll Buchanan United States Magistrate Judge

Judge's signature

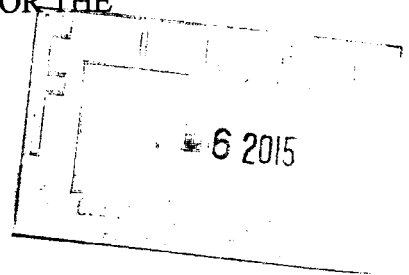
The Honorable Theresa C. Buchanan U.S. Magistrate Judge

Printed name and title

City and state: Alexandria, VA

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA)
)
 v.) No. 1:15mj515
)
 ARDIT FERIZI,)
 a/k/a "Th3Dir3ctorY,")
)
 Defendant.)

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

Kevin M. Gallagher, being duly sworn, says:

I. INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since August 2009. I am currently assigned to the Washington Field Office. I have training in the preparation, presentation, and service of criminal complaints and arrest and search warrants, and have been involved in the investigation of numerous types of offenses against the United States, including crimes of terrorism, as set forth in 18 U.S.C. § 2331 *et seq.* Prior to my current employment, I was an independent contractor for approximately three years, working as an intelligence analyst for two other government agencies within the intelligence community. My knowledge about this investigation comes from my personal participation in this investigation, a review of documents, electronic media, e-mails, and other physical and documentary evidence, and interviews of witnesses. I have also relied on information provided to me by other agents and law enforcement officials in the United States. Where statements of others are set forth, they are set forth in substance and in part. Because this affidavit is being submitted for the limited purpose

of establishing probable cause for the requested warrant, it does not contain all information known to me or to the government relating to this investigation.

2. Ardit Ferizi, aka “Th3Dir3ctorY” (“FERIZI”), a Kosovo citizen residing in Malaysia, is believed to be the leader of a known Kosovar internet hacking group, Kosova Hacker’s Security (“KHS”). In or about April 2015, FERIZI used the Twitter account @Th3Dir3ctorY to provide unlawfully obtained personally identifiable information (“PII”) to an Islamic State of Iraq and the Levant (“ISIL”) member, Tariq Hamayun (“Hamayun”), known as “Abu Muslim Al-Britani.” In addition, between in or about June 2015 and August 11, 2015, FERIZI provided unlawfully obtained personally identifiable information (“PII”) to a second known ISIL member, Junaid Hussain (“Hussain”), known as “Abu Hussain al-Britani.” On August 11, 2015, in the name of the Islamic State Hacking Division (“ISHD”), Hussain posted a public hyperlink on Twitter with the title “U.S. Military AND Government personnel, including Emails, Passwords, Names, Phone Numbers, and Location Information,” which provided ISIL supporters in the United States and elsewhere with the PII for over 1,000 U.S. government personnel, for the purpose of encouraging terrorist attacks against the identified individuals. Some of these individuals reside in the Eastern District of Virginia.

3. For the reasons detailed below, I submit that there is probable cause to believe that, from at least in or about April 2015 continuing through August 11, 2015, FERIZI gained unauthorized access to and obtained information from a protected computer, in violation of 18 U.S.C. § 1030. I further submit that there is probable cause to believe that, from at least in or about April 2015 continuing through on or about August 11, 2015, FERIZI used the unauthorized access to steal the means of identification and other personal information of U.S. military and other

government personnel, including their names, email addresses, passwords, and cities and states of residence, and then knowingly possessed and transferred the means of identification and other stolen information with the intent to aid or abet unlawful activity constituting a violation of federal law, particularly a felony violation enumerated in 18 U.S.C. § 2332(g)(5)(B), all in violation of 18 U.S.C. § 1028A(a)(2). Specifically, the PII stolen by FERIZI was knowingly provided to ISIL to be used by ISIL members and supporters to conduct terrorist attacks against the U.S. government employees whose names and locations were published. Prior to that, in or about April 2015, FERIZI transferred PII containing credit card information to ISIL. Based on the information contained in this Affidavit, I believe FERIZI conspired, attempted to provide, and provided, material support to ISIL, a designated foreign terrorist organization, in violation of 18 U.S.C. § 2339B.

4. I expect that FERIZI will be arrested outside of the United States and will be first brought to the Eastern District of Virginia.

II. BACKGROUND REGARDING ISIL AND JUNAID HUSSAIN

5. On October 15, 2004, the U.S. Department of State designated Al-Qa'ida in Iraq, then known as Jam'at al Tawhid wa'al-Jihad, as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist Entity pursuant to Executive Order 13224.

6. On May 15, 2014, the U.S. Department of State amended the designation of Al-Qa'ida in Iraq ("AQI") as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist Entity under Executive Order 13224 to list the name Islamic State of Iraq and the Levant ("ISIL") as its primary

name. The Department of State also added the following aliases to the ISIL listing: the Islamic State of Iraq and al-Sham (ISIS), the Islamic State of Iraq and Syria (ISIS), ad-Dawla al-Islamiyya fi al-‘Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furqan Establishment for Media Production. Although the group has never called itself “Al-Qa’ida in Iraq (AQI)”, this name has frequently been used by others to describe it. To date, ISIL remains a designated FTO. In an audio recording publicly released on or around June 29, 2014, ISIL announced a formal change of its name to the Islamic State.

7. On or about September 21, 2014, ISIL spokesperson Abu Muhammad al-Adnani called for attacks against citizens, civilian or military, of the countries participating in the United States-led coalition against ISIL.

8. Junaid Hussain, also known by the *nom de guerre* or *kunya* Abu Hussain al-Britani, was a British hacker and well-known member of ISIL. On or about August 24, 2015, Hussain was killed in an airstrike in Raqqah, Syria, a city which I know ISIL considers to be its capital.¹

III. RELEVANT LAW

9. I am advised that 18 U.S.C. § 1030(a)(2)(C) provides:

Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished [not more than five years].

10. Also, I am advised that section 1030(a)(7) provides:

(a) Whoever with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication concerning any—threat, [to damage a protected computer, to obtain information without

¹<http://www.centcom.mil/en/news/articles/iraq-progresses-in-isil-fight-key-extremist-confirmed-dead>

access, or demand or request money or other thing of value in relation to damage to a protected computer], . . . shall be punished [not more than five years].

A “computer” is defined as 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. The term “protected computer” includes a computer which is used in or affecting interstate or foreign commerce or communication. 18 U.S.C. § 1030(e)(1) and (e)(2)(B).

11. I am also advised that 18 U.S.C. § 1028A(a)(2) provides:

Whoever, during and in relation to any felony violation enumerated in section 2332(g)(5)(B) [defining Federal crimes of terrorism], knowingly transfers, possesses, or uses, without lawful authority, a means of identification [as defined in 18 U.S.C. § 1028(d)(7)] of another person. . . [shall be guilty of a separate felony].

12. Additionally, I am advised that 18 U.S.C. § 2339B provides:

Whoever knowingly provides material support or resources to a foreign terrorist organization,² or attempts or conspires to do so, shall be [guilty of a felony]. To violate this paragraph, a person must have knowledge that the organization is a designated terrorist organization (as defined in subsection (g)(6)), that the organization has engaged or engages in terrorist activity (as defined in section 212(a)(3)(B) of the Immigration and Nationality Act), or that the organization has engaged or engages in terrorism (as defined in section 140(d) (2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989.

“Material support or resources” means “any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safe houses, false documentation or identification, communications

² I am advised that the term “terrorist organization” means an organization designated as a terrorist organization under section 219 of the Immigration and Nationality Act. 18 U.S.C. § 2339B(g)(6). As stated above, ISIL is a designated foreign terrorist organization (“FTO”).

equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials.

“Expert advice or assistance” means advice or assistance derived from scientific, technical or other specialized knowledge. 18 U.S.C. §§ 2339A(b)(1), (b)(3) & 2339B(g)(4).

IV. STATEMENT OF PROBABLE CAUSE

A. FERIZI IS Th3Dir3ctorY

13. On April 5, 2015, @Th3Dir3ctorY, using the name “Ardit Ferizi,” publicly tweeted a link to a June 2013 article from the InfoSec Institute,³ as shown in the screenshot below:



Photo: Screenshot of FERIZI/@Th3Dir3ctorY's April 5, 2015 Tweet with a link to the June 2013 InfoSec Institute Article on KHS and @Th3Dir3ctorY

14. According to the interview of Th3Dir3ctorY by the InfoSec Institute, the user of Twitter account @Th3Dir3ctorY is the leader of a group of ethnic Albanian hackers from Kosovo, calling themselves Kosova Hacker's Security (“KHS”), which is responsible for

³ The InfoSec Institute (www.infosecinstitute.com), founded in 1998 and based in Illinois, is a training institute for technology professionals focused on information assurance, information technology auditing, database, project management, coding and related vendor training. InfoSec Institute also publishes research and articles, including interviews with hacking organizations.

compromising government and private websites in Israel, Serbia, Greece, the Ukraine, and elsewhere.

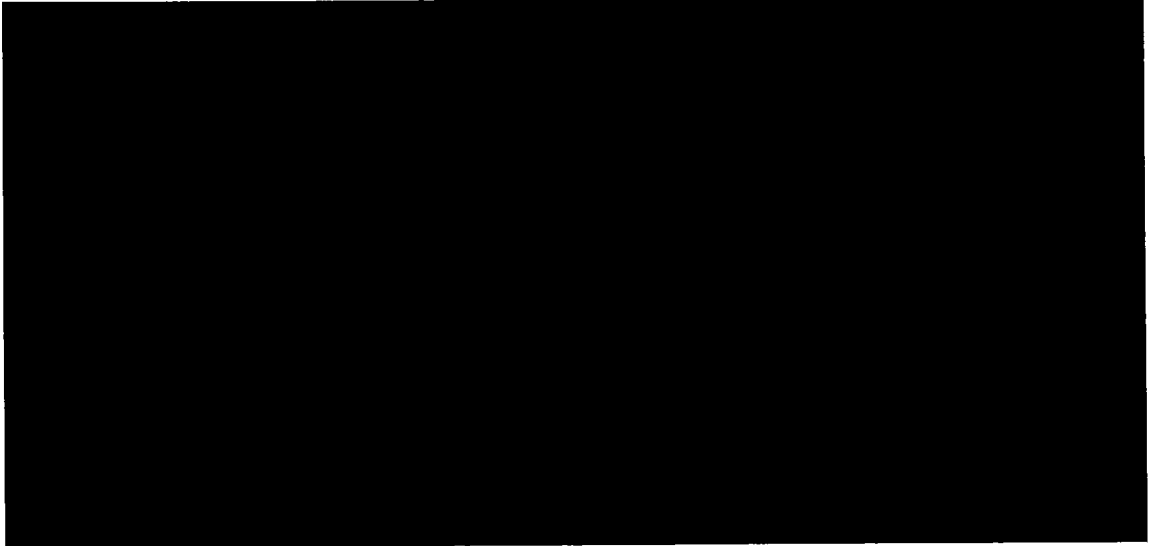


Photo: Banner for “Kosova Hackers Security” (KHS)

15. According to the article, as of the time of publication, KHS claimed responsibility for having hacked more than 20,000 websites, including: 90% of Serbian government websites; Interpol, based in France (including taking its site down for two days) in October 2012; and IBM’s research domain, researcher.ibm.com, located in Somers, New York, in May 2012. KHS also claimed responsibility for having posted more than 7,000 Israeli credit card numbers in January 2012. Again according to the article, hackers calling themselves “Th3Dir3ctorY” and “ThEta.Nu” also claimed responsibility for compromising Microsoft’s Hotmail servers in 2011. KHS itself has confirmed its involvement in these attacks in other open sources.

16. On or about July 10, 2015, @Th3Dir3ctorY posted a tweet identifying himself as “Owner of Kosova Hacker’s Security, Pentagon Crew,” and again used the name Ardit Ferizi:



Photo: Screenshot of @Th3Dir3ctorY's Twitter profile as of July 10, 2015

17. According to Twitter records, the @Th3Dir3ctorY account was registered on September 1, 2012, using Microsoft email account lajmetal@hotmail.com, from an Internet Protocol⁴ address allocated to IPKO Telecommunications LLC in Albania, a telecommunications company that provides services in the adjacent country of Kosovo. This registration information is consistent with @Th3Dir3ctorY's association with KHS, an organization which claims to be associated with Kosovo. Moreover, the investigation has revealed that FERIZI is a citizen of Kosovo.

⁴ Devices directly connected to the internet are identified by a unique number called an Internet Protocol, or IP, address. This number is used to route information between devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. In other words, an IP address is similar to a phone number, and indicates the online identity of the communicating device. IP addresses are allocated by an international organization, the Internet Assigned Numbers Authority.

18. Based on my investigation, I know that FERIZI currently resides in Malaysia on a student visa and that, as of spring 2015, FERIZI was studying at Limkokwing University in Malaysia. I believe that FERIZI entered Malaysia in or about early 2015.

19. IP logs for Twitter account @Th3Dir3ctorY reveal that all logins to @Th3Dir3ctorY between June 15, 2015 and August 14, 2015 originated with internet service providers (“ISPs”) in Malaysia.

B. ABU MUSLIM AL-BRITANI, A MEMBER OF ISIL, IS THE USER OF TWITTER ACCOUNT @MUSLIM_SNIPER_D

20. The Twitter account @Muslim_Sniper D came to the attention of the FBI following the May 2015 shooting incident at the “Draw Mohammad Contest” in Garland, Texas. On May 3, 2015, two roommates from Phoenix, Arizona, Elton Simpson and Nadir Soofi, fired at a security guard outside the contest venue. Garland police fired back, and when one of the two men pulled out what appeared to be a hand grenade, police shot and killed both men. Based on my investigation, including my review of publicly available social media postings, I believe that Simpson and Soofi were supporters of ISIL.

21. Twitter records demonstrate that the user of @Muslim_Sniper D had been in communication with @atawaakul, a Twitter account believed to have been used by Simpson, prior to the May 3, 2015 incident, and that the two users had discussed issues of “security.”

22. According to those records, the user of @Muslim_Sniper_D publicly identified himself as “Tariq Hamayun.” According to my investigation, Hamayun, 37 years old, was a car mechanic who volunteered for the Taliban and fought in Pakistan before joining ISIL in Syria.

Twitter records confirm that @Muslim_Sniper_D, originated from an ISP providing service in Raqqah, Syria.

23. On April 21, 2015, Hamayun, using Twitter account @Muslim_Sniper_D, published a tweet that read: “God Willingly will be making the best Electronics LAB in the Islamic state, would be producing sophisticated IEDs.”

24. On April 22, 2015, Hamayun, using Twitter account @Muslim_Sniper_D, published a tweet that read: “IEDs is my favourite weapon after Sniping, u hit the enemy & disappear in thin air just like a Ghost. Its [sic] a Must.”

C. FERIZI’S TRANSFER OF PII TO ISIL MEMBER ABU MUSLIM AL-BRITANI

25. On or about April 26-27, 2015 there was a Twitter exchange between the accounts @Muslim_Sniper_D and @Th3Dir3ctorY. During this exchange, FERIZI, as the user of @Th3Dir3ctorY, provided Hamayun, the user of @Muslim_Sniper_D, with screen shots of what appears to be unlawfully obtained credit card information belonging to 27 Americans, 18 British and 22 French citizens, including: names; addresses; zip codes; birth dates; and credit card information, such as the type, number, expiration date and Card Verification Value. Based on the context of this exchange, I believe that FERIZI provided this information intending it to be used by and for ISIL.

26. In the conversation, FERIZI asked the user of @Muslim_Sniper_D to confirm that he was “speaking with britani :) abu britani :)” to which Hamayun replied, “Yes brother/Im muslim al britani.” Hamayun moreover confirms his association with “Abu Hussain Al-Britani,” which is, as described above, the *nom de guerre* of ISIL member Junaid Hussain, who was based in Syria. Hamayun told FERIZI that Abu Hussain al Britani (Junaid Hussain) “is my friend he told

me a lot about u.” This exchange indicates that as of on or about April 26, 2015, FERIZI and Hussain were already in communication with one another.

27. At the end of this exchange, the user of @Muslim_Sniper_D, Hamayun, wrote the following message to the user of Twitter account @Th3Dir3ctorY, FERIZI:

“Pliz [sic] brother come and join us in the Islamic state.” (Emphasis added.)

D. FERIZI’S TRANSFER OF PII TO ISIL MEMBER ABU HUSSAIN AL-BRITANI

28. On August 11, 2015, Hussain, using Twitter account @AbuHussain_16, re-tweeted a post from the Twitter account @IS_Hacking_Div, which had, in the name of the Islamic State Hacking Division (“ISHD”), publicly tweeted a link to PII belonging to approximately 1,351 U.S. military and other government employees. As detailed below, there is probable cause to believe that FERIZI provided these 1,351 names to ISIL.

29. On or about June 13, 2015, FERIZI accessed without authorization a protected computer, namely a server (“Victim Server”) belonging to an identified internet hosting company (the “Hosting Company”), which maintained the website belonging to a U.S. retailer that sells goods via the internet to customers in multiple states (“Victim Company”). The Victim Server is physically located in Phoenix, Arizona. Some of the customers whose information was obtained reside in EDVA. Based on my conversations with other FBI agents, it is a dedicated server, meaning that no companies other than the Victim Company utilize this server. The Victim Server is leased by the Victim Company and owned by the Hosting Company.

30. FERIZI subsequently used his unauthorized access to the Victim Server to obtain the PII of approximately 100,000 people. Sometime between June 13, 2015 and August 11, 2015, FERIZI provided the PII of approximately 1,351 U.S. military and other government personnel to

ISIL, intending it to be used by and for ISIL, and knowing that ISIL would use the PII against the U.S. personnel, including to target the U.S. personnel for attacks and violence. Earlier, in or about March 2015, ISHD, acting in the name of ISIL, posted a “Kill List” including the purported names and addresses of 100 American service members.

31. On August 11, 2015, Hussain re-posted the following tweet by IHSD:

“NEW: U.S. Military AND Government HACKED by the Islamic State Hacking Division!”

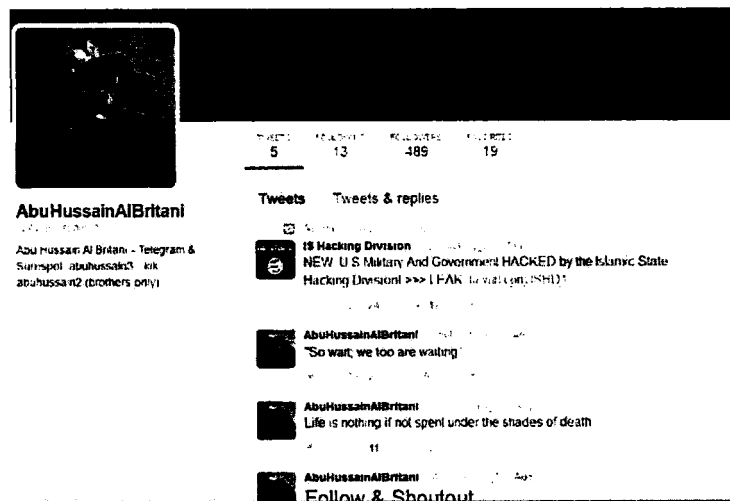


Photo: Screenshot of @AbuHussain_16 (Abu Hussain Al Britani) Twitter profile as of August 11, 2015

32. The tweet contained a hyperlink to a 30-page document. The beginning of the document warned the “Crusaders” who were conducting a “bombing campaign against the muslims” . . . that “we are in your emails and computer systems, watching and recording your every move, we have your names and addresses, we are in your emails and social media accounts, we are extracting confidential data and passing on your personal information to the soldiers of the khilafah, who soon with the permission of Allah will strike at your necks in your own lands!” The next 27 pages of the document contained the names, e-mail addresses, e-mail passwords, locations,

and phone numbers for approximately 1,351 U.S. military and other government personnel. The final three pages of the document contained what appear to show (i) credit card numbers and addresses for three federal employees and (ii) Facebook exchanges between U.S. military members. One of the Facebook exchanges includes what appears to be a discussion between two service members (“Service Member-1” and “Service Member 2”). Under this exchange, the creator of the document wrote, “Went to Iraq and returned in a body bag – Hell is the abode of the disbelievers . . .” Based on my review of public-source documents, I know that Service Member-1, a veteran of combat in Iraq and Afghanistan, was in fact killed in 2008, albeit in an accident after returning to the United States.

E. FERIZI’S FIRST KNOWN OFFER OF HACKING-RELATED ASSISTANCE TO ISIL ASSOCIATES

33. The April 26-27, 2015 communication in which FERIZI sent PII to Hamayun was not the first in which FERIZI communicated with ISIL members/supporters and offered them his computer expertise. On April 19, 2015, using @Th3Dir3ctorY, FERIZI posted a publicly available tweet directed to ISIL-affiliated accounts, which read: “@the_traveler01 @ksasisti @AbuBakrSShani brother wait till im [sic] making the script which u can upload and never get deleted (DEDICATED SERVERS)” [.]



Ardit Ferizi
- Th3Dir3ctorY

⚙️ Follow

@the_traveler01 @ksasisti @AbuBakrSShani
brother wait till im making the script which u
can upload and never get deleted
(DEDICATED SERVERS)

6:06 PM - 19 Apr 2015

Photo: Screen shot of the April 19, 2015 Tweet by FERIZI aka @Th3Dir3ctorY showing FERIZI's intent to support ISIL.

34. I believe this tweet reflects FERIZI's intention to create and provide a "script," or computer program aimed at assisting ISIL to publicly post communiqués and/or propaganda in a fashion which would supposedly make it difficult for such content to be removed by service providers or law enforcement.

35. All three accounts referenced in the above tweet by @Th3Dir3ctorY have been suspended by Twitter (date unknown). Based on searches of cached tweets, all appear to contain pro-ISIL messages, possibly explaining the suspensions. For example, on April 18, 2015, according to a public posting on pastebin⁵ (<http://pastebin.com/NBAs8mcU>), Twitter user @the_traveler01, utilizing the name "Abu Naseeha," was suspended by Twitter after posting the Al-Furqan/ISIL video of beheadings of Christians and Kurdish Pershmerga. On April 18, 2015, Twitter user @AbuBakrSShani "re-tweeted" the following by @Liberation_X, a pro-ISIL Twitter account: "RT @Liberation_X Egypt Sinai 3high ranking army commanders join islamic state in

⁵ Pastebin is a web application where users can store plain text. They are most commonly used to share short source code snippets for review via Internet Relay Chat.

Sinai.” In April 2015, @ksasisti tweeted: “Muwahideen⁶ of Shaytat tribe denounce & declare their enmity to the people from their blood who've allied with Assad,” followed by another tweet which read: “They also ask Sh Abubakr Baghdad⁷ to let them fight the filth from their tribe who allied with Bashar Assad.”

F. FERIZI IS THE SOURCE OF THE HACKED PII HE SENT TO ISIL

36. On August 13, 2015, an employee of the Victim Company reported an unauthorized access to their website. More specifically, the employee contacted an FBI agent and informed the agent that an account using the username “KHS,” which I believe to be an acronym for Kosova Hackers Security, had access to customer details from their databases. According to the Victim Company, customer information stored in the database included: names, addresses, cities, states, countries, phone numbers, email accounts, and usernames and passwords.

37. On August 17, 2015, the FBI was provided with an exchange between an employee of the Victim Company and technicians at the Hosting Company that owns the server on which the Victim Company’s website resides.

38. According to the exchange, beginning as early as June 13, 2015, an unauthorized user gained access to the Victim Company’s website, and created a user account with the initials KHS.

39. During an exchange that occurred on July 15, 2015, the Hosting Company technician verified to the Victim Company that the Hosting Company was witnessing ongoing

⁶ *Muwahideen* is an alternate spelling for “mujahedeen” or “mujahideen,” a term used to describe guerrilla fighters in Islamic countries, especially those who are fighting against non-Muslim forces. In this instance, I believe it is used to refer to those who fight for ISIL.

⁷ Abu Bakr al Baghdadi is the leader of ISIL.

outbound cyber-attacks against their infrastructure. The Hosting Company verified that the attacks were originating from the account utilizing username "KHS" and provided information about the account, discussed below.

40. According to the "Password last set" entry, which states "**6/13/2015 7:28:19 AM**," I believe the account was created on or before June 13, 2015. According to the "Last logon" entry, at **7/15/2015 11:32:01 AM**, I believe KHS had accessed the Victim Server as recently as the day of the exchange between the Victim Company and the Hosting Company.

```
C:\Users\Administrator>net user KHS
User name KHS
Full Name KHS
Comment
User's comment
Country code 000 (System Default)
Account active Yes
Account expires Never
Password last set 6/13/2015 7:28:19 AM
Password expires Never
Password changeable 6/13/2015 7:28:19 AM
Password required Yes
User may change password Yes
Workstations allowed All
Logon script
User profile
Home directory
Last logon 7/15/2015 11:32:01 AM
Logon hours allowed All
Local Group Memberships *Administrators *Users
Global Group memberships *None
```

41. The Hosting Company also identified that the file being run by KHS on July 15, 2015 was DUBrute.exe, located at the following directory:

```
C:\Users\KHS\Desktop\DUBrute v2.2 + VNC - Scanner GUI v1.2DUBrute v2.2
```

42. On August 19, 2015, the Victim Company contacted an FBI agent to report a threatening message it had received. The message, which was from an “Albanian Hacker,” with a contact email khs-crew@live.com, threatened the Victim Company for deleting the hacker’s “files” from their server. From my experience, I believe that the user of khs-crew@live.com was referring to the DUBrute.exe malware placed on the server which granted the user KHS unfettered access to information stored on the Victim Server.

43. The following is an excerpt of the email sent from an employee of the Victim Company to the FBI:

...I work for [owner of Victim Company] for his store [Victim Company].

The server was hacked again today and left a note on main page...⁸

Hi Administrator,

Is third time that your deleting my files and losing my Hacking JOB on this server !
One time i alert you that if you do this again i will publish every client on this Server!
I don't wanna do this because i don't win anything here !
So why your trying to lose my access on server haha ?
Why you're spending your time with one thing that you can't do ?
Please don't do the same mistake again because bad things will happen with you!
i didn't touch anything on your webhosting files please don't touch my files!
Want to contact me ?
Here : khs-crew@live.com

Greetings from an Albanian Hacker !

#SkyNet
#KHS

⁸ “Main page” refers to the primary page of the website operated by the Victim Company.

44. On August 20, an employee of the Victim Company wrote an email to khs-crew@live.com, identifying him/herself as an employee of the Victim Company, stating:

“Please dont attack our servers.” In response, the user of khs-crew@live.com wrote:

2BTC: 1f5Vgj7wMU9ofZWZno9ABsLSQ7XXkLsrG and will leave your server also make a report for method how am getting access to your servers :)

(Emphasis added.)

45. The employee replied “2 bitcoin mean? didnt get you whats that?” On August 21, 2015, the user of khs-crew@live.com sent a message to the Victim Company including information on what Bitcoins were and instructions on where the Victim Company should transmit the Bitcoin to:

<https://en.wikipedia.org/wiki/Bitcoin>

When i get money here : 1f5Vgj7wMU9ofZWZno9ABsLSQ7XXkLsrG

I will make full report for server and method .. i will protect and remove all bugs on your shop !

I believe that KHS demanded the two Bitcoin, worth approximately \$500, for KHS to relinquish his access to the Victim Server and to provide a report to the administrator on the method he was using to gain that access.

46. In August, the Victim Company provided the FBI with consent to review all information related to the Victim Company’s website, which is stored on the Victim Server owned by the Hosting Company.

47. FBI review of the image of the Victim Server reveals an originating IP address of 210.186.111.14. This is an IP assigned to a Malaysian-based ISP that is frequently used by FERIZI. The image shows that on July 8, 2015 at approximately 3:15 Universal Time Coordinate (UTC), the Victim Server was showing signs of a Structured Query Language (SQL) injection

attack. I learned from speaking with other FBI agents that SQL injection is a technique often used against retailer websites that inserts malicious code into a database entry field, thereby causing, for example, the database to send its content to the attacker. I believe that KHS has used this method of hacking in the past.

48. Records for Facebook account 100003223062873, associated with the vanity name "ardit.ferizi01," believed to be used by FERIZI, reveal that the account was accessed from the same IP responsible for the aforementioned SQL injection attack on the Victim Server on July 7, 2015 at approximately 06:49 UTC, the day prior to the initial unauthorized intrusion, and July 8, 2015 at approximately 12:34UTC, which is roughly six hours after the initial unauthorized intrusion.

49. Furthermore, FBI analysis of the Facebook records reveal over 1200 discrete actions attributed to IP 210.186.111.14 occurring between July 6, 2015 and July 13, 2015 including, but not limited to, account Logins, Session Terminations and sent messages.

50. Twitter records demonstrate that the @Th3Dir3ctorY account, attributed to FERIZI, was logged into from the same IP responsible for the SQL injection attack on the Victim Server at approximately 17:15 UTC the day prior to the initial unauthorized intrusion and at approximately 17:09 UTC on July 8, 2015, approximately 13 hours after the initial unauthorized intrusion.

51. Furthermore, FBI analysis of Twitter records reveal at least nine total logins to @Th3Dir3ctorY from IP 210.186.111.14 between July 5, 2015 and July 13, 2015.

52. FBI review of the Victim Server revealed that the full names, email addresses, passwords, and cities and states of residence for the 1,351 U.S. military and other government

personnel included in the release by Hussain and the ISHD on August 11, 2015 were found on the Victim Server.

53. On September 10, 2015, FERIZI sent himself, via Facebook, a file called `contact.csv`. FBI analysis shows that the data from file `contact.csv` (100,001 PII records) was imported into a spreadsheet and subsequently truncated to remove the trailing string characters followed by the “| (pipe)” symbol, so that the data could be compared against normal email address formats. For example, the data row `firstnamelastname@gmail.com|22483m` was truncated to remove “|22483m,” thus leaving “`firstnamelastname@gmail.com`,” which could then be used to compare against any matching email addresses from those posted online by ISIL on August 11, 2015. Utilizing this process, the records from the `.csv` file were reduced from approximately 100,000 to 98,890 records. The data was subsequently sorted and records not following normal email formats (*e.g.*, suffix “@xxx.xxx”) were removed. Any records not having a prefix before the @xxx.xx, were likewise removed. Additionally, all duplicative records were subsequently eliminated. There were 8,475 duplicate records, leaving 91,525 unique email addresses contained in the `.csv` file. The records from the Victim Server belonging to 1,351 customers of the Victim Company were then imported into the spreadsheet for comparison. In a similar manner, any duplicate email address records were eliminated, leaving 1,351 records which were subsequently compared against the 91,525 remaining email addresses contained in the `.csv`. Of the 1,351 unique records posted by ISIL on August 11, 2015, 1,089 records matched those records contained in the `.csv` file and 262 records did not match.

54. Furthermore, a review of the Facebook records revealed a conversation between FERIZI and another Facebook user, account “Butrint Komoni,” on or about August 22, 2015, in

which Facebook account Butrint Komoni asked FERIZI: “what happened with the [Victim Company’s website]” to which FERIZI replied, “the network came in :3. I called you man.” I believe FERIZI is confirming his unauthorized access to the Victim Server.

55. Given the above, I believe that FERIZI, the user of the Facebook account 100003223062873, obtained the PII belonging to the U.S. military and other government personnel by unlawfully accessing the Victim Server and provided that information to ISIL for ISIL’s use, including publication and for use against the owners of the PII.

V. CONCLUSION

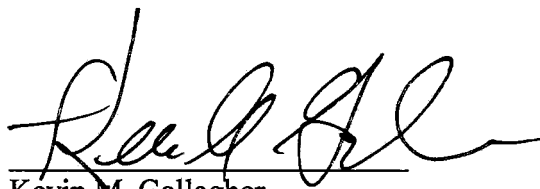
56. Based upon the facts detailed above, I respectfully submit that there is probable cause to believe that from on or about April 2015 to August 11, 2015, out of the jurisdiction of any particular State or district, Ardit FERIZI:

- a. Intentionally accessed the Victim Server, a protected computer, without authorization and exceeded authorized access to the Victim Server, and thereby obtained information from a protected computer, and the offense was committed in furtherance of a criminal act in violation of the laws of the United States, specifically, the criminal act of providing material support to a designated foreign terrorist organization as prohibited by 18 U.S.C. § 2339B, all in violation of Title 18, United States Code, Section 1030(a)(2) and (c)(2)(B)(ii);
- b. With intent to extort from persons money and other things of value, transmitted in interstate and foreign commerce a communication containing a threat to cause damage to a protected computer and threat to obtain

information from a protected computer without authorization and to impair the confidentiality of information obtained from a protected computer without authorization, all in violation of Title 18, United States Code, Section 1030(a)(7) and (c)(3)(A);

- c. Knowingly transferred, possessed and used, without lawful authority, a means of identification of another person (consisting of, among other things, names, birth dates, and credit card information) during and in relation to a felony violation enumerated in section 2332b(g)(5)(B), that is, providing material support to ISIL, a designated foreign terrorist organization as prohibited by 18 U.S.C. § 2339B, knowing that the means of identification belonged to another actual person, in violation of Title 18, United States Code, Section 1028A(a)(2).

d. Knowingly provided and conspired and attempted to provide material support to ISIL, a designated foreign terrorist organization, namely, property and services, including himself as personnel, expert advice and assistance in computer hacking, and the PII of U.S. military and government personnel, in violation of 18 U.S.C. § 2339B.



Kevin M. Gallagher
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
this 6 day of ~~September~~, 2015



Oct,

/s/

Theresa Carroll Buchanan
United States Magistrate Judge

The Hon. Theresa Carroll Buchanan
United States Magistrate Judge