UNITED STATES DISTRICT COURT

for the

District of Columbia

United States of America
v.
MIHAI ALEXANDRU ISVANCA
and
EVELINE CISMARU

Defendant(s)

Case No.

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 January 9 to January 12, 2017 in the county of Washington, DC in the _____ District of Columbia, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §§ 1349 and 1343	Conspiracy to commit wire fraud
18 U.S.C. §§ 371, 1030(a)(4), 1030 (a)(5)(A), 1030(a)(7), 1030(c)(3)(A) and (c)(4)	Conspiracy to commit unauthorized access of protected computers to commit fraud, to transmit programs to intentionally damage protected computers without authorization, and to transmit threats to damage protected computers in order to extort

This criminal complaint is based on these facts:

See Attached Affidavit.

☑ Continued on the attached sheet.

Complainant's signature

James Graham, Special Agent, U.S. Secret Service
Printed name and title

Sworn to before me and signed in my presence.

Date: 12/11/2017

Judge's signature

City and state: Washington, DC

Robin Meriweather,United States Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA **v.** **MIHAI ALEXANDRU ISVANCA** **AND** **EVELINE CISMARU** ***Defendants.***	**Case No.** **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, Special Agent James Graham, of the United States Secret Service, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service ("USSS"), Washington Field Office ("WFO"), and have been since June, 2015. I graduated from Saint Joseph's University with a Bachelor's Degree in Public Administration (International). My coursework included basic understanding in Accounting, Finance and Management. I have received a Graduate Certificate in Homeland Security from Texas A&M University. In 2013, I completed my Masters of Science in Security Studies with merit honors from the University College of London. This degree utilized quantitative and qualitative research methods to demonstrate a given issue in the Security Field of study.

2. Upon graduation from college, I worked as a USSS Uniformed Division Officer for six and a half years, during which time I dealt with complex physical premises access control methods and theories. Also, during this timeframe, I took one year of Leave Without Pay to pursue and graduate with my Master's Degree from the University College of London. In June 2015, I

attended the Federal Law Enforcement Training Center in Glynco, Georgia to complete my training in the Criminal Investigator Training Program ("CITP"). Here, I was taught the basics of conducting online investigations, including information sources for money transfers and for social media, as well as best legal practices when dealing with sites on the internet. After graduating from the Federal Law Enforcement Training Center, I attended agency specific training at The James J. Rowley Training Center in Beltsville, Maryland, where I became BICECP (Basic Investigation of Computers and Electronic Crimes Program) certified. In the BICECP program, I was provided in-depth training about the physical components of a computer, best practices for securing computer evidence, and potential evidence locations both on physical computer networks and on external sources (such as social networking sites). Further, while in training, I learned about various types of fraud, including credit card fraud schemes, typical methods of investigating credit card fraud, how credit card payment systems work, and sources of information.

3. After graduating from The James J. Rowley Training Center, I attended the USSS Network Intrusion Response Program, where I received in-depth training about network topologies, security measures, modern networking, and how to take an image of a computer. In addition, I received training on how to analyze an image to discover evidence relevant to an investigation (to include continually evolving, highly technical advanced malware), the attack steps involved in a network intrusion, the steps required in conducting a network intrusion investigation, proper questioning to determine relevant evidence upon analysis of a computer, Internet Protocol ("IP") addressing, internet anonymizers (such as proxies and VPNs), typical attack vectors in network intrusions, and proper documentation of network intrusions. I attended and completed the Point of Sale training, where I received training in the common points of attacks during a network intrusion of a given point of sale system. Also, I have completed the Hack-It and

Track-It training. In this training, we performed several different network attacks on a training virtual machine. After these network attacks were performed, forensic analysis would be performed to show identifiers of the performed network attack. In addition, I stay current with real time developments within the IT security field both through open source information as well as agency information sharing.

4. During my time as a Special Agent at the Washington Field Office, I have conducted numerous network intrusion investigations of businesses and entities within the National Capitol Region. As part of these investigations, I have conducted analyses on systems infected with malware and have observed the schemes, abilities, and methods of actors who have been successful in gaining unauthorized entry into systems.

5. This affidavit is submitted in support of a criminal complaint alleging that MIHAI ALEXANDRU ISVANCA ("ISVANCA") and EVELINE CISMARU ("CISMARU") (collectively, "the Defendants")

> FIRST, did knowingly and willfully combine, conspire, confederate and agree with each other and others known and unknown to the United States, to commit the following offense against the United States: with intend to defraud, to knowingly devise and intend to devise a scheme to defraud various persons in which, for the purpose of executing the scheme and attempting to do so, they would cause to be transmitted by means of wire communication in interstate commerce various signals and sounds constituting wire transmissions, in violation of 18 U.S.C. §§ 1349 and 1343; and
>
> SECOND, did knowingly and willfully combine, conspire, confederate and agree with each other and others known and unknown to the United States, to commit the following offenses against the United States: (1) to knowingly and with intent to defraud, access

protected computers without authorization and by means of such conduct to further their intended fraud and to obtain something of value; (2) to knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, to intentionally cause damage without authorization, to protected computers; (3) with intent to extort from persons money and other things of value, to transmit in interstate and foreign commerce communications containing threats to cause damage to protected computers and demands and requests for money and other things of value in relation to damage to protected computers, where such damage would be caused to facilitate the extortion, all in violation of 18 U.S.C. §§ 371, 1030(a)(4), 1030(a)(5)(A), 1030(a)(7), and 1030(c)(3)(A) and (c)(4).

6. This affidavit is based on my personal knowledge, information provided to me by other law enforcement agents, law enforcement records, email search warrant returns, witness interviews, and my training and experience, as well as on the training and experience of other law enforcement agents.

7. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause that the defendants violated, first, 18 U.S.C. §§ 1349 and 1343, and, second, 18 U.S.C. §§ 371, 1030(a)(4), 1030(a)(5)(A), 1030(a)(7), 1030(c)(3)(A) and (c)(4).

SUMMARY OF PROBABLE CAUSE

8. The evidence uncovered by the investigation shows that ISVANCA and CISMARU participated in a conspiracy to distribute ransomware by spam emails – that is, to send emails containing malicious software (also called malware) that would lock or encrypt files on various

victim computers to which the malware was to be sent and installed and, then, to extort money from the victims in exchange for unlocking or decrypting files on the computers. In furtherance of the conspiracy, between in or about January 9, 2017, and January 12, 2017, ISVANCA and CISMARU participated in an intrusion into and taking control of approximately 123 internet-connected computers used by the Metropolitan Police Department of the District of Columbia ("MPDC") to operate surveillance cameras in public, outdoor areas in the District of Columbia, which computers could then be used to send the ransomware-laden spam emails. Digital evidence on those surveillance camera computers reflects that unauthorized access and control for purposes of the ransomware scheme, as well as evidence of email accounts used by the co-conspirators. Those email accounts, in turn, reflect not just the ransomware scheme, but in various ways (and through related accounts and activity) ultimately identify ISVANCA and CISMARU as the participants in the conspiracy, including by leading back to email and other online accounts in their own names.

Intrusion of Surveillance Camera Computers

9. On or about January 12, 2017, the United States Secret Service ("USSS") learned that certain MPDC public surveillance cameras in the District of Columbia, had been disabled. Each disabled camera was controlled by a dedicated computer installed immediately adjacent to the camera and connected to a larger network and one or more servers operated by MPDC. The computers are "protected computers" under 18 U.S.C. §1030(e)(2) because the computers are "used in or affective interstate or foreign commerce or communication." The computers attached to the surveillance cameras are connected to the internet and are capable of being remotely accessed by MPDC or others working with or for MPDC.

10. On January 12, 2017, an MPDC information technology ("IT") network administrator showed USSS Special Agent Brian Kaiser that the MPDC IT staff was able to use a Remote Desktop Protocol ("RDP"), a standard tool available on nearly all computers running Windows software, to connect with any of the computers operating any of the surveillance cameras and thereby to observe real-time activity on those computers. Through the use of the RDP, Special Agent Kaiser could observe activity on a selected remote camera computer as if he were sitting in front of a monitor and directly operating that remote computer.

11. On January 12, 2017, the IT network administrator executed the RDP to access one of the surveillance camera computers ("Victim Device A") on the network. Victim Device A had a unique network IP address of 166.143.169.96, and was physically located in the District of Columbia. (An IP address is a unique number used by and/or assigned to a device that is connected to the internet; every computer attached to the internet must be assigned an IP address so that internet traffic sent from and directed to that computer may be directed properly from its source to its destination.) Upon execution of the RDP, Special Agent Kaiser personally observed activity on Victim Device A, including multiple open desktop windows on it. The computers were running software programs not installed by, and had files not saved or stored by, MPDC, all evidence that an intrusion – that is, unauthorized access and control – had occurred. These windows had not been opened by MPDC IT staff; rather, they had been opened by subject(s) who had acquired unauthorized access and control of the computer.

12. The opened desktop windows on Victim Device A included (a) a window displaying a tracking number for the European shipping company known as "Hermes"; (b) a web browser window open to https://app.sendgrid.com showing an activity feed for multiple email addresses; (c) a Google search page with search results for "email verifier online"; (d) a browser

window open to emailx.discoveryvip.com; (e) another window for a notepad program showing code for various executable files and text files; and (f) a window showing the splash screen for a variant of ransomware known as "cerber."

13. Based upon his observations, Special Agent Kaiser concluded that the subject(s) had gained unauthorized access to and control of Victim Device A. The IT network administrator confirmed that the subject(s) using that computer was/were not authorized to use the computer or the government network. The subject(s)'s network access was blocked thereafter.

14. Further investigation and analysis revealed that approximately 123 of the MPDC's 187 outdoor surveillance cameras had been accessed and compromised. Ultimately, three of those computers, including Victim Device A, were removed for forensic analysis by the USSS and the Federal Bureau of Investigation ("FBI").

15. USSS forensic analysts examined records and system logs recovered from two of the compromised computers, Victim Device A and Victim Device B, and FBI forensic analysts examined records and logs from the third computer, Victim Device C. Victim Devices B and C were also physically located in the District of Columbia. The examinations revealed that unauthorized access to and control and use of these three computers by the subject(s) occurred from about January 9 to January 12, 2017.

Ransomware Scheme

16. The analyses further revealed that two variants of sophisticated, malicious computer code had been placed on all three computers, one known as "cerber" and the other known as "dharma." From my training and experience, both forms of malicious code are used in ransomware schemes to lock victim computers on which the malware is installed and to extort

money from the computer owners in exchange for unlocking the computers. In addition, a text file, USA.txt, was found on Victim Device A which contained 179,616 email addresses.

17. The forensic analysis of the three computers revealed evidence that the computers had been and were intended to be used to distribute spam-mail in bulk containing the variants of the malicious code of "cerber" and "dharma" to the email addresses in the USA.txt file in order to promote a ransomware scheme.

18. As noted above at paragraph 12, Victim Device A had among other things a browser window open to https://app.sendgrid.com; the window also displayed the sendgrid.com account user name of "David Andrew." From my training and experience, I know that the website sendgrid.com is a commercially available bulk email service used by legitimate marketers to upload bulk email lists and distribute large quantities of email through its servers and by spammers to send large quantities of unwanted or malicious emails.

Ransomware Scheme – Evidence in Email Accounts, Including vand.suflete@gmail.com

19. Forensic analysis of Victim Device A determined that multiple email accounts had been accessed while the computer was under the control of the subject(s) between January 9 and January 12, 2017. Two such accounts were david.andrews2005@gmail.com and anonimano027@gmail.com.

20. Google records revealed that anonimano027@gmail.com had sent and received multiple emails with vand.suflete@gmail.com. ("Vand Suflete" translates from Romanian to English as "selling souls.") From my training and experience, individuals will use multiple email addresses so that criminal activities are not exposed or traced back to the originating person. One set of email correspondence appears to consist of test email on January 10, 2017, consisting of the subject line "x." In my training and experience, cyber criminals will send test emails to ensure

they are communicating with the correct account. Once they verify they are communicating with the correct account they will then send the information in question. These test emails were followed by another email on January 10 from vand.suflete@gmail.com to anonimano027@gmail.com included the IP addresses, usernames, and passwords for 94 of the IP addresses for MPDC surveillance camera computers confirmed to have been accessed and compromised, and additional IPs which appear to be on the same network. From my training and experience, I know that individuals will sometimes log into other IP addresses using that IP address' username and password, to create a degree of separation through a proxy server, thus making the criminal actions done on the IP address more difficult to be tracked back to them. In the email, listed next to various of the aforementioned IP addresses were the following (a) a reference to "cerber," a sophisticated form of ransomware; (b) "ars," a Romanian word for "burnt"; and "aici," a Romanian word for "here." "Aici" was listed next to the IP address 166.143.169.96, the IP address of Victim Device A. An email from vand.suflete@gmail.com to anonimano027@gmail.com identified various computers, by IP address, with corresponding usernames and passwords, which have been infected with or contain the code for the cerber variant of ransomware.

21. USSS agents contacted a number of persons or entities using the IP addresses mentioned in the email of the vand.suflete@gmail.com account regarding potential unauthorized access and compromise. One such victim, COMPANY M indicated they had experienced an unauthorized network intrusion. COMPANY M provided screenshots reflecting a cerber splashscreen from the period of unauthorized access, as well as multiple other indicators of network intrusion.

22. Google records for vand.suflete@gmail.com included an email with what is believed to be a link to a "cerber control panel." In my training and experience, within the cerber business model, the owner and creator of the cerber malware leases out cerber resources to affiliates (essentially, customers). A cerber control panel is a website that allows a cerber affiliate to control the cerber framework without having access to the source code, thereby allowing the owner and creator to retain for themselves the intellectual property of the malware and thus to generate additional income from other affiliates.

23. Google records for vand.suflete@gmail.com also included three emails from jokevanduijn@kpnmail.nl to vand.suflete@gmail.com, each containing files disguised as ".pdf" files that, when executed, requested the download of cerber malware. In my training and experience, such .pdf files with hidden links to download cerber malware are the types of files emailed to victims in ransomware schemes to lock victim computers on which the malware is installed and to extort money from the computer owners in exchange for unlocking the computers.

24. Google records for anonimano027@gmail.com included two emails confirming activation of a new account with the username "tommy tommy" on the website IFUD.WS, a known cyber-criminal forum. During the investigation, Special Agent Kaiser accessed the IFUD.ws hack forum and found a username "tommy tommy" (user number 18105). On January 11, 2017, "tommy tommy" posted a topic theme named "Cerber one of the best ways to make money in 2017," written in English, which post contained the following: "Looking for and rdp suppliers who wants to work for cerber virus on a good % Add me for more details tommy.tommy@jabber." No additional comments or posts by tommy tommy were visible on the forum. IFUD.WS profile details for username tommy tommy include a Jabber ID of tommy.tommy@jabber.ru with ICQ

number 717259811, a username registration date of January 11, 2017, a date of birth of January 1, 1989, showing a sex of female.

25. Google records for vand.suflete@gmail.com included an email received from "noreply@jabber.ru" confirming the registration of the jabber account "tommy.tommy@jabber.ru" referenced in the IFUD.WS post seeking individuals "who wants to work for cerber virus on a good %."

Ransomware Scheme – Evidence Linked to eveline.cismaru@gmail.com

26. Google records for vand.suflete@gmail.com included multiple email exchanges with eveline.cismaru@gmail.com. In one such email exchange, eveline.cismaru@gmail.com sent an email to vand.suflete@gmail.com containing an individual's personal identifying information, including a full name, a physical address, and an email address; in a reply email, vand.suflete@gmail.com account stated, "succes parola la cont pe site e," which roughly translates from Romanian to English as "successful password to your account on the site is," followed by what appears to be a password. In addition, there are multiple emails sent from vand.suflete@gmail.com to eveline.cismaru@gmail.com containing IP addresses and what appear to be usernames and passwords for a given IP address. This is similar in style to the January 10 email from vand.suflete@gmail.com to anonimano027@gmail.com which included the IP addresses, usernames, and passwords for 94 of the IP addresses for MPDC surveillance camera computers.

27. Google records for eveline.cismaru@gmail.com included a January 10, 2017, email sent to david.andrews2005@gmail.com containing the file USA.txt, which had been previously forwarded by suhm2006@hotmail.com on January 9, 2017. As noted above at paragraph 16, the file USA.txt (containing 179,616 email addresses) was also found on Victim Device A. The MD5

checksum calculated on the USA.txt file located on Victim Device A matches the MD5 checksum calculated on the USA.txt file found in the eveline.cismaru@gmail.com account. A checksum is a computer algorithm run by forensic analysts on two or more files found in an investigation in order to determine if they match. Since a checksum algorithm will output a significantly different value if the input is changed, the checksum can be used to determine if the file or files found on separate pieces of evidence are the same file or have been modified. Generally, changing the name of a file will not affect the file's checksum value, while changing the contents inside the file will. In laymen's term, the match here means that the USA.txt file is the exact same file on Victim Device A and in the eveline.cismaru@gmail.com account.

Ransomware Scheme – Evidence Linked to amisvanca@gmail.com

28. Google records revealed that amisvanca@gmail.com was listed as a recovery email address by the anonimano027@gmail.com registrant. A recovery email account is sometimes required when registering an email address so as to allow the owner of the account to regain access in the event of a lost, stolen, or otherwise compromised password. The recovery account would therefore be critical to reestablishing access to the main account. From my training and experience, I know that it is extremely unlikely that a user would provide another person's email address such that the user would not have control over the recovery address.

Other Evidence Linked to vand.suflete@gmail.com, eveline.cismaru@gmail.com, amisvanca@gmail.com

29. Google records for these accounts included several emails sending and receiving credit card information. In various emails, amisvanca@gmail.com sent and/or received information pertaining to approximately 1,603 credit cards; eveline.cismaru@gmail.com sent and/or received information pertaining to approximately 2,170 credit cards; and

vand.suflete@gmail.com sent and/or received information pertaining to approximately 55 credit cards.

Evidence Linked to Window Observed on Victim Device A – Hermes delivery

30. Investigation of the Hermes tracking number (referenced above at paragraph 12, as observed on Victim Device A) by the National Crime Agency ("NCA") of the United Kingdom ("UK") reflected a delivery address in London and an email address. The execution of a warrant at that address resulted in two residents being detained. Both denied involvement and forensics analysis of their seized media revealed no evidence inculpating them in the offenses described herein.

31. The IP address (77.95.34.172) used to create the Hermes order, as observed on Victim Device A, was an IP address registered to a healthcare company in the United Kingdom. (Google records for vand.suflete@gmail.com included a December 19, 2016, email containing a reference to that IP address, that is, a line of text which read as follows: 77.95.34.172:3389@WELLWORK\XAFServiceAccnt;citrixA9#%abcABC.) When contacted by the NCA, the company stated it had confirmed evidence of unauthorized access to its computer servers and had located a user account on its system named "XAF Service Account" that they believed had been compromised. The company stated it was a user profile that contained files and information that appeared related to "Bitcoin, email sender software, mailbot programs along with some text files that indicate the presence of Ransomware programs." The company provided access to server logs which showed remote access to their server, including unauthorized access by the IP address 188.25.175.248 multiple times between January 2 and January 10, 2017 and by the IP address 86.107.57.138 twice on January 10, 2017.

Further Evidence Regarding ISVANCA

32. As noted above at paragraph 28, Google records for anonimano027@gmail.com (accessed from Victim Device A) revealed that amisvanca@gmail.com was listed as a recovery email address by the anonimano027@gmail.com registrant. Google records revealed that the anonimano027@gmail.com account was created on January 10 or 11, 2017, with the terms of service IP address (that is, the IP address used by the account holder at the time of the account creation) of 86.107.57.138. As also noted above at paragraph 31, that IP address was also used to remotely access computer servers of a healthcare company in the United Kingdom, which servers were used in the ransomware scheme.

33. Google records for david.andrews2005@gmail.com (also accessed from Victim Device A) showed that account was created on January 5, 2017 with the same terms of service IP address of 86.107.57.138.

34. Google records also revealed a January 9, 2017 email to david.andrews2005@gmail.com with an invoice from callcenter@andys-pizza.ro, reflecting a food delivery to "mihai alexandru" located at "bucur 4-6, 4-6, ap. 26, entrance 026, floor 5, Bucharest." Additional USSS research on the address revealed that the individual residing at the address since 2013 was Ovidiu Alexandru Dan. Dan was arrested in 2016 by Bucharest law enforcement for skimming related crimes (understood to mean crimes involving the theft of financial account identifiers for credit and debit cards). He was indicted at the end of 2016 and his case was pending at the Bucharest Court at the time of the USSS research.

35. On March 8, 2017, the NCA reported that a fraud database query on the email david.andrews2005@gmail.com included results showing that an individual named Mihai Alexandru Isvanca, a Romanian national, was associated with the email address through a number

of transactions that were flagged as suspicious due to the fact that the billing address did not match the shipping address.

36. Google records for amisvanca@gmail.com revealed that when the account was created on February 26, 2014, the name given during registration was Alexandru Mihai. The email account name itself also relates to Alexandru Mihai Isvanca.

37. Google records for vand.suflete@gmail.com revealed that the account was accessed numerous times from IP address 86.107.57.138, dating back to October 14, 2016, and include ten times on January 2, 2017, alone. Google records included an email to vand.suflete@gmail.com that names the account as Alexandru Mihai; this email also includes numerous IP addresses and what appears to be corresponding login information for these IP addresses.

38. Pursuant to a Mutual Legal Assistance Treaty ("MLAT") request to the Romanian Police, investigators obtained records related to IP address 86.107.57.138 showing that the IP address was a static IP address through Teen Telecom and was set up for the period October 2016 to January 2017 under the name of Mihai-Alexandru Isvanca. The Teen Telecom records also listed a telephone number of 0726192907, an email address of a_isvanca@yahoo.co.uk, and an address of "Bacau, Bld. Oituz, nr 33, sc B, Ap. 17." From my training and experience, I know that a static IP address is assigned by a provider to the customer; while a dynamic IP address is assigned by the network and as a result, will likely change with time.

39. An open source query (*i.e.*, search) on Facebook of amisvanca@gmail.com resulted in a profile of "Alexandru Mihu." No photos were publicly available in that account/profile. From my training and experience, I know that individuals will often perform slight alterations on their names on social media to disguise their identities. Facebook profile "Eveline Dima" listed and

tagged a Facebook profile "Alex Isvanca." This "Alex Isvanca" profile showed two separate pictures of a male and listed that he lives in the United Kingdom. These pictures appear to be the same individual pictured in a photo of ISVANCA provided by the Romanian Police through the NCA.

40. Romanian Police through the NCA provided the following passport and public records information about ISVANCA:

Name: Mihai Alexandru Isvanca
Date of Birth: 08 November 1992
Romanian Unique ID: 1921108045369
Romanian Passport Number: 55260582 (issued 06 November 2017)

Further Evidence Regarding CISMARU

41. Related to the two London residents at the address related to the Hermes tracking number observed on Victim Device A (as described above at paragraphs 12, 30, and 31), their attorney provided information from Amazon showing that they made a purchase through Amazon from a "Lakel" company. The Lakel company contact information used the email address eveline.cismaru@gmail.com.

42. Google records for eveline.cismaru@gmail.com showed that the account was registered on February 1, 2015, under the name "eveline vblog" and had a terms of service IP address of 87.117.204.166. The records also showed that the recovery email address for this account was eveline.cismaru@hotmail.com.

43. Google records also revealed several emails between eveline.cismaru@gmail.com and vand.suflete@gmail.com with what appeared to be login information of a given network, utilizing its IP address, username, and password.

44. Google records also included several emails to eveline.cismaru@gmail.com, addressing the account user as “Eveline Cismaru” or “Eveline.” This included airline booking receipts and tickets, emails regarding potential housing, and an application for a driver’s license in the United Kingdom. Also, an email from eveline.cismaru@gmail.com to Airbnb inquired about an account deactivation and stated at the end, “kind Regards Eveline Cismaru.”

45. A Facebook query of eveline.cismaru@gmail.com resulted in an “Eveline Dima” account and a later query resulted in a “Diana Millan” account. A further query into these profiles revealed that these two profiles are listed as friends with one another. From my training and experience, I know that individuals will often times perform slight alterations to a profile name on social media to disguise and prevent other individuals from locating them. The photos posted on the Eveline Dima Facebook profile appeared to be of the same person as the pictures found in the eveline.cismaru@gmail.com account. Also, the same picture of the same person appeared on the Eveline Dima Facebook profile and within an email of the eveline.cismaru@gmail.com account. Within the Eveline Dima Facebook profile, investigators observed a picture of an Apple laptop captioned “business time.” These aforementioned photos appeared to be of the same person when compared to a passport photo of CISMARU provided by the Romanian Police through the NCA.

46. Another item shown on the Eveline Dima Facebook profile is a YouTube video from the YouTube profile of “eveline vblog.” The corresponding YouTube channel of “eveline vblog” included several videos of the individual from the same Facebook profile of Eveline Dima. Google records for eveline.cismaru@gmail.com included an email received from YouTube in regards to a comment on a video from the “eveline vblog” channel. From my training and experience, I know that the account holder on YouTube will receive emails in regards to comments on their videos and other activities regarding their respective Youtube channel.

47. Romanian Police through the NCA provided the following passport and public records information about CISMARU:

Name: Eveline Cismaru
Date of Birth: 01 October 1989
Romanian Passport Number: 052347613 (issued 25 April 2014)
Driver's License (United Kingdom) Application Number: 20161811726971
Government Gateway User ID (United Kingdom): 4911 3765 7479

CONCLUSION

Wherefore, based upon the foregoing, there is probable cause to believe that MIHAI ALEXANDRU ISVANCA and EVELINE CISMARU between January 9, 2017 and January 12, 2017, and continuing thereafter to a date not known by the affiant, in the District of Columbia and elsewhere,

FIRST, did knowingly and willfully combine, conspire, confederate and agree with each other and others known and unknown to the United States, to commit the following offense against the United States: with intend to defraud, to knowingly devise and intend to devise a scheme to defraud various persons in which, for the purpose of executing the scheme and attempting to do so, they would cause to be transmitted by means of wire communication in interstate commerce various signals and sounds constituting wire transmissions, in violation of 18 U.S.C. §§ 1349 and 1343; and

SECOND, did knowingly and willfully combine, conspire, confederate and agree with each other and others known and unknown to the United States, to commit the following offenses against the United States: (1) to knowingly and with intent to defraud, access protected computers without authorization and by means of such conduct to further their intended fraud and to obtain something of value; (2) to knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, to intentionally cause damage without authorization, to protected computers; (3) with intent to extort from persons money and other things of value, to transmit in interstate and foreign commerce communications containing threats to cause damage to protected computers and demands and requests for money and other things of value in relation to damage to protected computers, where such damage would be caused to facilitate the extortion, all in

violation of 18 U.S.C. §§ 371, 1030(a)(4), 1030(a)(5)(A), 1030(a)(7), and 1030(c)(3)(A) and (c)(4).

Respectfully submitted,

_____
James Graham, Special Agent
United States Secret Service

Subscribed and sworn to before me on _____, 2017

_____
HON. ROBIN M. MERIWEATHER
UNITED STATES MAGISTRATE JUDGE