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

UNITED STATES OF AMERICA

v.

PETER ROMAR
(a/k/a "PIERRE ROMAR")

&

FIRAS DARDAR
(a/k/a "THE SHADOW"),

Defendants.

Criminal No. 1:15-MJ-498

UNDER SEAL

AFFIDAVIT IN SUPPORT OF
CRIMINAL COMPLAINT AND ARREST WARRANTS

I, Patrick DiMauro, being first duly sworn, hereby depose and state as follows:

BACKGROUND AND OVERVIEW OF THE CONSPIRACY

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) assigned to the Washington Field Office, Washington, D.C., and I have been personally involved in the investigation of this matter. I have been employed by the FBI as a Special Agent since 2010. Throughout my FBI employment, I have received training in general law enforcement and in specialized areas including national security computer intrusions. As a Special Agent of the FBI, I am authorized to investigate crimes involving computer intrusions, national security, and other crimes stated under federal law, including Title 18 of the United States Code.

2. I make this affidavit in support of an application for a criminal complaint charging PETER ROMAR (also known as "PIERRE ROMAR") and FIRAS DARDAR (also known as "THE SHADOW") with violation of the following federal laws: (1) conspiracy to

commit unauthorized computer intrusions, in violation of Title 18, United States Code, Section 1030(b); (2) conspiracy to commit money laundering, in violation of Title 18, United States Code, Section 1956(h); (3) conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349; (4) conspiracy to violate the Syrian Sanctions Regulations, in violation of Title 50, United States Code, Sections 1705(a) and (c); and (5) conspiracy to violate multiple federal laws under Title 18, United States Code, Section 371, including 18 U.S.C. § 880 (receiving the proceeds of extortion), and 18 U.S.C. § 875(d) (sending an unlawful interstate communication).

3. As discussed in more detail below, defendants DARDAR and ROMAR are skilled computer hackers who have worked on behalf of the Syrian Electronic Army (SEA), a group that has been involved since at least in or about 2011 in a number of well-publicized computer intrusions in support of the Syrian regime and to punish perceived detractors of Syrian president Bashar al-Assad.

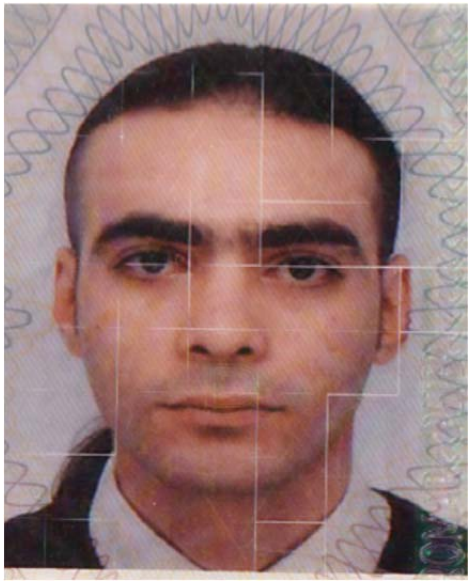
4. In addition to those intrusions, the investigation has revealed that since at least in or about late 2013, DARDAR and ROMAR have been involved in unlawful computer intrusions for monetary gain through the targeting and compromising of computer systems located in the United States and elsewhere, and extortion of victims, with DARDAR sometimes touting his SEA affilation. In executing this scheme, DARDAR conducted computer intrusions from his location in Syria and sent threats and demands for payment to each victim, and ROMAR, from his location in Germany, received and attempted to retransmit the extortion proceeds to SEA members in Syria, in violation of U.S. sanctions against Syria.

5. The facts in this affidavit come from my personal observations, my training and experience, information obtained from other agents and witnesses, and my examination of

reports, records, and other evidence. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

The Defendants

6. Defendant ROMAR is a Syrian national currently residing in Waltershausen, Germany. This is an image of ROMAR:



As set forth in greater detail below, ROMAR controlled the email account pierreromar.mail@gmail.com and the Facebook, Inc. (Facebook) account "pierre.romar1" (Facebook account ID number 100005382097823), and used those accounts in furtherance of the criminal activities described herein:

A. pierreromar.mail@gmail.com: A review of records obtained from a court-authorized search warrant confirms that the pierreromar.mail@gmail.com account was controlled by ROMAR. Among other things, the account contained multiple emails in

which ROMAR attached a scanned copy of his German passport, including the photograph depicted above, as well as multiple emails containing photographs of ROMAR, job applications for ROMAR, and outgoing correspondence signed by ROMAR under his true name.

B. Facebook account "pierre.romar1" (ID number 100005382097823): In addition to the fact that the user selected an account name that is a variation of ROMAR's alias (PIERRE ROMAR), subscriber information for the account confirms that the account is controlled by the user of pierreromar.mail@gmail.com, namely ROMAR. As discussed later in this affidavit, the contents of this Facebook account, obtained by a court-authorized search warrant, further confirm that ROMAR controlled this account, as the contents of communications with co-conspirator DARDAR over this Facebook account are consistent with the contents of contemporaneous communications between ROMAR's pierreromar.mail@gmail.com account and DARDAR's accounts listed below.[1]

[1] Communications between ROMAR, DARDAR and an SEA hacker known as "Th3 Pr0" (discussed in further detail in this affidavit), were usually conducted in Arabic, and I have reviewed draft translations of those communications.

7. Defendant DARDAR is a Syrian national and a resident of Homs, Syria. This is an image of DARDAR:

As set forth in greater detail below, DARDAR controlled the email accounts sea.the.shadow@gmail.com, ethicalspectrum@gmail.com, and codezero70@gmail.com, as well as a Facebook account (ID number 100006770461994), all of which he used in furtherance of the criminal activities described herein:

A. sea.the.shadow@gmail.com: A review of records obtained from a court-authorized search warrant confirms that the sea.the.shadow@gmail.com account was controlled by DARDAR. Among other things, the account contained emails in which the user of the account sent scanned attachments of identification documents issued by the Syrian Ministry of the Interior, including DARDAR's personal identifiers, and the account regularly received incoming correspondence addressing the recipient as "Feras Dardar" or "Firas Nour Alden Dardar." In addition, on multiple occasions DARDAR sent emails from this account to his hacking victims that included photographs depicting

his banking information (so that victims could send money to him as part of the extortion scheme), which consistently listed his name as the beneficiary of the account.

B. ethicalspectrum@gmail.com: Subscriber records obtained from Google confirm that this account was controlled by the user of sea.the.shadow@gmail.com, namely DARDAR. Further, a court-authorized search of the ethicalspectrum@gmail.com account revealed that DARDAR also used that account to send his hacking victims the same photograph depicting his banking information that he had also sent from his sea.the.shadow@gmail.com account. The search also revealed that DARDAR used ethicalspectrum@gmail.com to transmit images of his Syrian Government-issued identification card and an English translation of that card.

C. codezero70@gmail.com: A review of records obtained from a court-authorized search warrant confirms that this account was controlled by DARDAR. Specifically, on or about January 7, 2015, the user of this account sent an email with an attached signed contractual agreement in DARDAR's name, as well as a copy of one of the same official Syrian identification documents that DARDAR transmitted over his sea.the.shadow@gmail.com account. Further, the account contained communications with hacking victims dated between in or about July 2014 to in or about January 2015, in which the user of the account directed victims to transfer extortion payments to bank accounts maintained under DARDAR's name.

D. Facebook account (ID number 100006770461994): The user of Facebook account 100006770461994 registered it using the first name "Sea" and the last name "The-Shadow," a reference to DARDAR's hacker pseudonym (THE SHADOW) and his affiliation with the SEA. Further, as discussed below in this affidavit, the contents of

Facebook chats between ROMAR and Facebook account 100006770461994 confirm that DARDAR controlled it, as the conversations discuss, and coincide with, activity seen in ROMAR and DARDAR's email communications.

PROBABLE CAUSE

Background to the SEA's Hacking Activities

8. DARDAR, using the online alias THE SHADOW, and another Syrian hacker known as "Th3 Pr0" are notorious members of the Special Operations Division of the SEA, a group of computer hackers responsible for computer intrusions intended to punish perceived detractors of Bashar al-Assad, the president of Syria, and to publish pro-Assad propaganda.

9. Among other computer intrusion methods they utilized, SEA hackers sent phishing emails to victims that purported to come from a trusted source and that contained hyperlinks to websites appearing to be trusted websites, but which actually were controlled by the hackers.[2] A recipient who clicked on these hyperlinks was directed to a conspiracy-controlled website that mimicked a legitimate, trusted website. The recipient was then asked for credentials, such as a username and password, for access to the supposedly trusted website. In the intrusion attacks that were successful, at least one recipient provided his or her credentials when prompted, thus unknowingly providing those credentials to the hackers. The SEA hackers then used the stolen credentials to obtain unauthorized access to the computer systems of the target entity. Once these systems were accessed, SEA hackers would conduct a variety of malicious activities, including but not limited to redirecting legitimate Internet traffic, defacing

[2] "Phishing" is the act of attempting to acquire information, such as usernames and passwords, by masquerading as a trustworthy entity in an electronic communications. "Spearphishing" consists of "phishing" attempts directed at specific individuals or companies. Attackers may gather personal information about their target to increase their likelihood of success.

and altering website text, sending messages using the victim's accounts, and conducting further phishing attempts.

10. Beginning at least in or around 2011, the individuals and entities targeted by DARDAR and Th3 Pr0 on behalf of the SEA included: Harvard University, the Washington Post, the White House, Reuters, Human Rights Watch, National Public Radio, the Associated Press, CNN, The Onion, NBC Universal, Inc., USA Today, the New York Post, the National Aeronautics and Space Administration (NASA), and the Microsoft Corporation.

ROMAR Affiliates with the SEA

11. As a result of the SEA's hacking activities, DARDAR and Th3 Pr0 gained notoriety under their online hacker pseudonyms. In or about April 2013, ROMAR contacted Th3 Pr0 via Facebook regarding ROMAR's attempts to affiliate himself with the SEA. Search warrant returns from ROMAR's Facebook account indicate that between on or about April 11, 2013, and April 28, 2013, ROMAR engaged in a conversation with a Facebook account used by Th3 Pr0 (Facebook account 100005539625632, vanity name "Th3Pro.Net.Sy," registered to "ViVa ThePro"). In this conversation, ROMAR indicated that he had reached out to Th3 Pr0 approximately five months previously "about working with [him]" and noted that he had provided Th3 Pr0 with information about computer intrusions that ROMAR had conducted in the past (stating that he had provided a "record of [his] hackings"). ROMAR asked Th3 Pr0 for assistance with a cyberattack that ROMAR was planning against entities located in Saudi Arabia, Turkey, and Qatar.

12. In response to ROMAR's request for assistance with computer hacking operations, Th3 Pr0 arranged an introduction between DARDAR and ROMAR. Search warrant returns from sea.the.shadow@gmail.com indicate that on or about April 28, 2013, Th3 Pr0

provided DARDAR with the website URL[3] for ROMAR's Facebook account (www.facebook.com/pierre.romar1) and instructed DARDAR to "[h]elp him, whatever he needs". On or about April 29, 2013, Th3 Pr0 directed ROMAR to contact DARDAR for assistance, providing ROMAR with the URL of DARDAR's Facebook account (www.facebook.com/SEA.Th3.Shad0w). Later that day, DARDAR added ROMAR as a Facebook friend.

Overview of DARDAR and ROMAR's Hacking and Extortion Scheme

13. Starting in at least approximately late 2013, DARDAR began using his computer hacking skills and notoriety as an SEA hacker to expand the goal of his activities beyond support of the Syrian regime, to personal monetary gain through computer intrusion and extortion schemes. As described in detail below, DARDAR committed unlawful computer intrusions into private companies in the United States and elsewhere and, in at least one instance, used his notoriety and affiliation with the SEA to instill fear in victim companies and extort money from them. Further, ROMAR played an important role in the scheme by helping to transmit the extortion proceeds from victim companies to Syria, which was necessary because DARDAR had difficulty obtaining funds directly as a result of U.S. and other countries' sanctions against Syria. ROMAR did so with the knowledge that he was receiving funds from the victims of DARDAR's hacking activities and that he was assisting DARDAR in evading the relevant sanctions.

14. Based upon, among other things, a review of the contents of email and Facebook accounts used by ROMAR and DARDAR, information provided by victims of the scheme, and other documentary evidence, the investigation has identified at least approximately 14 different

[3] "URL" stands for "Uniform Resource Locator," which is a protocol for specifying addresses on the Internet. It is an address that identifies a particular file on the Internet and usually consists of the protocol, typically represented as "http," followed by the website domain name.

U.S. and international victims of the extortion scheme between in or about July 2013 and in or about December 2014. DARDAR demanded in total more than $500,000 from those 14 victims as part of the extortion element of the scheme, although ROMAR and DARDAR accepted smaller amounts in many circumstances. The details uncovered by the investigation regarding seven of the victims are discussed in detail below.

The Unlawful Objects of the Conspiracy

15. In conducting the malicious computer intrusion activities and illicit financial transactions described herein, DARDAR and ROMAR violated multiple U.S. criminal statutes. Those statutes include:

A. 18 U.S.C. § 1030(b): conspiracy to commit and aid and abet computer intrusions in violation of the Computer Fraud and Abuse Act (CFAA), with the unlawful objects of: (i) unauthorized access of a computer and obtaining information (18 U.S.C. § 1030(a)(2)); (ii) unauthorized access of a computer to defraud and obtain value (18 U.S.C. § 1030(a)(4)); (iii) causing unauthorized damage to a computer (18 U.S.C. § 1030(a)(5)); and (iv) transmitting extortionate threats relating to damaging a computer (18 U.S.C. § 1030(a)(7));

B. 18 U.S.C. § 1956(h): conspiracy to commit money laundering, with the unlawful objects of: (i) promoting the carrying on of a specified illegal activity (18 U.S.C. § 1956(a)(1)(A)(i)); (ii) concealing or disguising the nature of the proceeds of the specified unlawful activity (18 U.S.C. § 1956(a)(1)(B)(i)); and (iii) promoting the carrying on of a specified illegal activity through the transmission or transfer of funds from a place in the United States to or through a place outside the United States (18 U.S.C. § 1956(a)(2)(A));

C. 18 U.S.C. § 1349: conspiracy to commit wire fraud;

D. 50 U.S.C. § 1705(a): conspiracy to violate the Syrian Sanctions Regulations (31 C.F.R. § 542.207); and

E. 18 U.S.C. § 371: conspiracy with the unlawful objects of: (i) receiving the proceeds of extortion (18 U.S.C. § 880), and (ii) sending an unlawful interstate communication (18 U.S.C. § 875(d)).

Manner and Means of the Conspiracy

16. Some of the methods of the Conspiracy for infiltrating computer systems and extorting victims to further its unlawful goals can be summarized as follows:

A. A member of the Conspiracy obtained unauthorized access to a victim company's computer systems, including by sending phishing emails to employees of that company.

i) A conspirator, in many instances DARDAR, designed an email meant to entice the recipient into clicking on a hyperlink embedded in the message.

ii) A conspirator, in many instances DARDAR, sent these emails to the intended victims.

iii) Recipients that clicked on the hyperlink in the phishing email were asked for login credentials, such as their username and password, for their accounts on legitimate computer systems. For the attacks that were successful, at least one recipient was deceived into providing his or her credentials to the Conspiracy.

iv) A conspirator, often DARDAR, then used the legitimate credentials without authorization to access the victim computer systems.

B. Once the victim company's computer systems were accessed, a member of the Conspiracy would redirect legitimate Internet traffic to or from the victim's systems, deface and alter website text, send messages using the victim's accounts, attempt further phishing attempts, exfiltrate data, or engage in other illegitimate activities.

C. DARDAR would then send emails from one of his above-listed personal accounts to employees of the victim entities that indicated his responsibility for the hack and provided proof of the system compromise. DARDAR would then demand payments from the victim and make threats about what would happen if payment was not received, including threats that he would cause further damage to the victim's systems, or sell information stolen from the victim to other hackers.

D. ROMAR, who resides in Germany, would receive funds from victims who could not transmit money directly to DARDAR and other conspirators in Syria due to the sanctions against Syria, all with the knowledge that he was receiving funds from the victims of his co-conspirators' hacking activities and that he was assisting DARDAR and other conspirators in Syria in evading the relevant sanctions.

Extortion Attempts and Overt Acts

17. A member of the Conspiracy committed at least the following extortion attempts and, in furtherance of the Conspiracy, at least the following overt acts, with at least one overt act occurring in the Eastern District of Virginia (see Paragraph 45 below):

I. VICTIM 1, an Online Gaming Company, Is Extorted

18. In or about July 2013, DARDAR obtained unauthorized access to the computer systems of VICTIM 1, a Chinese online gaming company, which operates its online services from U.S.-based servers. On or about July 24, 2013, DARDAR, using the sea.the.shadow@gmail.com account, sent several emails to employees of VICTIM 1 in which he informed the recipients in sum and substance that he had hacked one of its games, and demanded payment. DARDAR threatened VICTIM 1 in the course of his demands and noted, in an email dated on or about July 24, 2013, that "[t]his is the last warning / communicate with me or / I will did [sic] something you do not like."

19. Email correspondence reveals that VICTIM 1 made its first payment of $500 to DARDAR via Perfect Money[4] shortly thereafter. Following that payment, DARDAR regularly sent emails to representatives of VICTIM 1 claiming to have identified other vulnerabilities in VICTIM 1's servers for which he extracted additional payments or gaming privileges.

20. On or about November 18, 2013, a representative of VICTIM 1 sent an email that informed DARDAR that his information regarding additional vulnerabilities was proving to be of little value. DARDAR responded by indicating that he had access to all of VICTIM 1's databases ("i have Access on everything and i have everything") and demanded €50,000 in exchange for the databases. VICTIM 1 confirmed that DARDAR had indeed accessed its systems, but attempted to get DARDAR to agree to installment payments of €1,333 rather than a large, one-time sum. DARDAR rejected the proposal, noting that he had compromised VICTIM 1's server for a long period of time ("in your server from 3 month . . .work inside your server is

[4] Perfect Money is an online e-commerce payment system, which allows users to transmit funds online.

easyer [sic] than out of it"), and he threatened to cause damage to VICTIM 1 ("do every thing can [sic] to hurt you."). DARDAR eventually lowered his extortionate demand to €15,000.

21. Over the course of the next five months, DARDAR sent additional messages to representatives of VICTIM 1 in which he described additional hacks into VICTIM 1's systems, and DARDAR demanded further payments which he referred to as "blackmail." DARDAR, in the course of his communications with representatives from VICTIM 1, occasionally mentioned his affiliation with the SEA and the fact that he was wanted by the FBI.

22. During the course of his email communications with VICTIM 1, DARDAR mentioned the difficulties he encountered receiving money in Syria as a result of sanctions. Specifically, DARDAR stated that "[b]anks in Syria does [sic] not accept dollar" and that "[British] banks refused to send money to Syria."

II. VICTIM 2, a U.K.-based Web Hosting Company, Is Extorted

23. In or about October 2013, DARDAR obtained unauthorized access to the computer systems of VICTIM 2, a U.K.-based web hosting company. On or about October 20, 2013, DARDAR, referring to himself as "Shadow," his SEA hacker pseudonym, sent an email from sea.the.shadow@gmail.com to a representative of VICTIM 2 in which he claimed to be an "ethical hacker" and requested payment of €50,000 for assisting VICTIM 2 in avoiding future hacks. Further, DARDAR threatened to use VICTIM 2's servers to conduct unlawful computer intrusions on other victim systems if VICTIM 2 did not comply with his demands for payment.

24. As in his dealings with VICTIM 1, DARDAR experienced difficulty receiving proceeds of the extortion of VICTIM 2 as a result of sanctions against Syria. Specifically, e-mail correspondence between DARDAR and representatives of VICTIM 2 indicate that they settled on a payment of €15,000 to satisfy DARDAR's demands. DARDAR sent a photograph of his

banking information to Victim 2, which listed his name ("FIRAS DARDAR") as the beneficiary of the account. However, when VICTIM 2 attempted to send DARDAR the payment via an American Express international payment system, the transaction was rejected because the beneficiary bank was in Syria. An employee of VICTIM 2 informed DARDAR that the payment transaction had been rejected and indicated that "[t]he us has a trade imbargo [sic] . . . ."

25. Based on email correspondence, over the course of the extortion DARDAR apparently managed to obtain a total of at least approximately €16,000 from VICTIM 2 through payments made from the United Kingdom directly to Syria.

III. VICTIMS 3 and 4, Web Hosting Companies, Are Extorted

26. During late 2013, DARDAR successfully compromised computer systems belonging to a Europe-based web hosting company (VICTIM 3), and a dedicated server and web hosting company based in California (VICTIM 4). As detailed below, DARDAR enlisted ROMAR's assistance to transmit the proceeds of extorting both VICTIM 3 and VICTIM 4 to Syria.

27. VICTIM 3: On or about October 29, 2013, DARDAR sent an e-mail to employees of VICTIM 3 from his sea.the.shadow@gmail.com account, and informed them that he had "hacked [VICTIM 3's] websites servers and databases" and "downloaded it all." DARDAR provided images to prove that he had successfully compromised the company's systems, and noted that he had two buyers who would each pay €150,000 for the stolen data. Further, DARDAR demanded €300,000 in exchange for refraining from further attacks and releasing valuable information obtained during the penetration, and for a report on how he executed the attack.

28. The next day, a representative of VICTIM 3 replied to DARDAR and attempted to negotiate a lower price. After DARDAR made threats of further intrusions, damage, and that he would sell VICTIM 3's data, VICTIM 3 informed DARDAR that its bank would not process payments directly or indirectly to Syria due to sanctions against the country.

29. VICTIM 4: On or about November 27, 2013, DARDAR, using the ethicalspectrum@gmail.com account, sent a threatening email to several employees of VICTIM 4 stating, "if you d[o]n't respond[,] like many companies didn't respond [to] this message . . . , i will hack your website/s . . . ." and, "if i haven't receive[d] any respon[se,] i'm sorry because i will use your database and your servers [for] my work[.] you have just 1h to respond[.]" He touted his hacking abilities, noting that "you have no idea about my skills." When VICTIM 4 failed to respond to his initial threat, DARDAR compromised the company's domain registration account and modified the routing information for the company's and some of its clients' websites. As a result of this compromise, Internet traffic to such sites was redirected to a Conspiracy-controlled website bearing the following message:

HACKED

> I told you [expletive deleted] don't [expletive deleted] with me go now and cry like a little bitch you and your [expletive deleted] CEO all your data downloaded and one of it has been sold ... I offer all of the databases for sale for just $100.

30. The next day, on or about November 28, 2013, a representative of VICTIM 4 sent an email to DARDAR and asked what they could do to convince DARDAR to relinquish control over the re-directed domains. DARDAR responded and demanded that €100,000 be deposited into his bank account and an additional €5,000 be sent to him via Perfect Money. DARDAR threatened to sell information regarding vulnerabilities in VICTIM 4's systems to other hackers

if the company failed to comply with his demands.[5] On or about December 6, 2013, the representative of VICTIM 4 informed DARDAR by email that VICTIM 4's bank was "giving [VICTIM 4] a hard time" sending money to DARDAR in Syria, but that he was investigating other forms of electronic payment systems to provide funds to DARDAR, including PayPal,[6] Bitcoin, and Webmoney. DARDAR replied that none of those payment systems were available to him in Syria.

31. On or about December 15, 2013, DARDAR enlisted ROMAR to assist him with receiving the proceeds of the extortion scheme from VICTIM 3 and VICTIM 4, because he was having trouble receiving the funds in Syria. Specifically, DARDAR raised the issue with ROMAR over Facebook, informing ROMAR that he needed assistance in transferring money because it was "stuck in [European location of VICTIM 3] and America." DARDAR further stated that he was receiving payments as a result of computer hacking activities, explicitly noting that he had hacked VICTIM 3. DARDAR indicated that if he did not receive payment from VICTIM 3, he would "declare a war on them." ROMAR responded in part by agreeing to assist DARDAR with the transfer of funds, and DARDAR told ROMAR to expect "about 1450 Euros."

32. As discussed below, on the same day that ROMAR agreed to help DARDAR receive the proceeds of extortion from VICTIM 3 and VICTIM 4, DARDAR reached out to representatives of both VICTIM 3 and VICTIM 4 and made arrangements to have the extortion payments made through ROMAR in Germany.

---

[5] A review of the contents of DARDAR's ethicalspecturum@gmail.com account reveals that DARDAR attempted to sell information to at least five different hackers on the same date.

[6] PayPal is an online payment system which provides users with the ability to transfer funds electronically between individuals and businesses.

33. On or about December 15, 2013, DARDAR instructed VICTIM 3 by email to "please send the money to Peter Romar[ ]in Germany via western union." On or about December 20, 2013, after receiving no reply from VICTIM 3, DARDAR responded with threats in an email entitled "important I hacked your servers":

> I will take your not responding is a breach of the Convention
> So I have the right to do what I want with the information
>
> I did to you a favor and you have to pay it back
> or i will take it by my self
>
> As you know, we (Ethical Hackers) have a reputation and we must maintain it
> , I did not took [sic] much time to hack your servers
> But I assure you I will provide plenty of time to I [sic] recover my right
> Note:
> You have one day to respond
> If you do not respond
> ..... ?? :)

VICTIM 3 responded by indicating its willingness to pay DARDAR, but that it had earlier indicated that it required a signed contract, accompanied by a copy of the signatory's passport, before it would process any payments. On or about December 27, 2013, DARDAR responded that his "friend" would send the required contract.

34. On December 30, 2013, ROMAR emailed VICTIM 3 from his pierreromar.mail@gmail.com account, which included a contract and a scanned image of ROMAR's German passport.

35. Approximately three days later, as part of DARDAR's efforts to facilitate the payment from VICTIM 3, DARDAR forwarded ROMAR an email with no new text, but which included in the email chain the text of the email quoted above in paragraph 33, entitled "important I hacked your servers." Accordingly, based on my training and experience, and my familiarity with this investigation, I believe that ROMAR had access to the entirety of the email

chain and was aware of the specific threats that DARDAR made regarding VICTIM 3's computer systems if VICTIM 3 did not comply with making extortion payments through ROMAR.

36. Between on or about January 3, 2014, and on or about March 24, 2014, DARDAR and the CEO of VICTIM 3 exchanged emails pertaining to: (a) the status of the signed contracts and their delivery from ROMAR in Germany to VICTIM 3's offices in Europe; and (b) DARDAR's possession of an image of the CEO's passport, which DARDAR claimed to have obtained as a result of hacking into the CEO's email account. DARDAR demanded an additional €50,000 from VICTIM 3 in exchange for information concerning how he obtained the image of the CEO's passport.

37. A February 18, 2014 email from VICTIM 3 to DARDAR indicates that VICTIM 3's bank refused to send money to ROMAR because of ROMAR's Syrian nationality. VICTIM 3 offered to open a new account at a bank that would not have issues with ROMAR's nationality and asked DARDAR to reduce the extortion payment of €5,000 in an effort to reduce difficulties with the new bank. DARDAR agreed.

38. On or about March 24, 2014, a representative of VICTIM 3 emailed DARDAR and asked him to arrange for ROMAR to sign a nondisclosure agreement. DARDAR forwarded the agreement to ROMAR by email and stated as follows:

> He wants you to sign this contact to protect the secrecy of the information
> Read it and if there is something you don't agree on let me know
> You have to sign the two pages, scan them and send them to me.

39. Approximately two days later, ROMAR emailed DARDAR at sea.the.shadow@gmail.com, addressed him as "The Shadow," and attached a scan of the agreement bearing ROMAR's signature and address in Germany.

40. On or about April 22, 2014, VICTIM 3 emailed DARDAR and informed him that it had received confirmation that €5,000 was sent to the "German bank account."

41. As discussed above in paragraph 30, as of on or about December 6, 2013, a representative of VICTIM 4 had informed DARDAR, in sum and substance, that VICTIM 4's bank would not allow it to send funds to DARDAR in Syria. On or about December 15, 2013, DARDAR sent an email to the representative of VICTIM 4 and instructed him to send the money to "Peter Romar in Germany." Approximately four days later, on or about December 19, 2013, the representative of VICTIM 4 replied and indicated that he would send the funds through Western Union. In subsequent correspondence, the representative from VICTIM 4 indicated that approximately $1,500 was sent, and requested confirmation of receipt.

42. On or about December 25, 2013, DARDAR subsequently forwarded the email correspondence with VICTIM 4 regarding the Western Union payment from his sea.the.shadow@gmail.com account to ROMAR at pierreromar.mail@gmail.com. As part of that email, DARDAR instructed ROMAR to transmit €1450 to SEA hacker Th3 Pr0 ("1450 EUR / /Send it to / [Th3 Pr0's real name]").

43. Also on or about December 25, 2013, ROMAR and DARDAR had discussions using their respective Facebook accounts identified above, which covered the same topics, including: (1) identifying the name of the executive from VICTIM 4 who was responsible for sending the Western Union payment; and (2) verifying that funds should be transmitted to Th3 Pr0 in Syria.

44. Records obtained from Western Union confirm that on or about December 27, 2013, ROMAR received a Western Union payment from VICTIM 4 of approximately $1,500, before fees. ROMAR simultaneously communicated with DARDAR using Facebook and

informed DARDAR that he had forwarded the amount left after fees to an intermediary in Lebanon, whom ROMAR had instructed to forward the money to Th3 Pr0. ROMAR further indicated that he had to use this circuitous route because his local Western Union office would not forward the money directly to Syria due to "new law." Prior Facebook conversations between DARDAR and ROMAR, which occurred no later than December 15, 2013, indicate that ROMAR was aware of sanctions against Syria, and that those sanctions prevented German banks from wiring money to Syrian banks.

IV. VICTIM 5, a U.S.-based Online Media Company, Is Extorted

45. According to a representative of an online media company with offices in the United States (VICTIM 5), VICTIM 5's computer systems were compromised by a spearphishing attack that occurred on or about March 7, 2014. Based on my review of records provided by VICTIM 5 and interviews of its employees, I know that as a result of the spearphishing attack, the attackers obtained unauthorized access to VICTIM 5's computer servers and databases, including a server located in Ashburn, Virginia, within the Eastern District of Virginia. The attackers also hijacked social media accounts belonging to VICTIM 5, accessed VICTIM 5's PayPal account, attempted to withdraw funds from the PayPal account, and defaced websites belonging to VICTIM 5.

46. On or about March 8, 2014, the day following the compromise, an employee at VICTIM 5 received messages from a compromised Google account belonging to VICTIM 5 in which the sender took responsibility for the hack. In those communications, the hacker demanded €15,000 in exchange for him stopping "the hack" against the company and for refraining from selling the company's database or erasing information from the company's computer systems. Further, the hacker instructed the employee to send the €15,000 to DARDAR ("Feras Nour Eddin Dardar") in Syria.

47. Later, DARDAR sent further instructions to an executive of VICTIM 5 from the ethicalspectrum@gmail.com account. In e-mail correspondence between DARDAR and the executive between on or about March 8, 2014, and on or about March 10, 2014, the executive indicated that he had attempted to transmit funds to DARDAR, but that Western Union would not permit him to send money to Syria. The executive further stated that attempts to transfer funds from a U.S.-based bank account failed because, as the executive explained to DARDAR, "[i]t is illegal and not possible to send money from the US to Syria, you probably should know that for future hacks." After the executive attempted to persuade DARDAR to not retaliate against VICTIM 5, DARDAR continued to make threats, including, "I should break my promise too then i must to hack and destroy and ... etc / And then your losses will be greater than my losses doubles."

48. On or about March 19, 2014, after not receiving the demanded payment from VICTIM 5, DARDAR followed through with his threats. DARDAR used the stolen VICTIM 5 customer email lists to distribute spam emails to thousands of VICTIM 5's customers. These emails advertised the sale of VICTIM 5's databases – "hacked by ethical spectrum" – for €5000. According to representatives of VICTIM 5, the incident cost the company tens of thousands of dollars, but VICTIM 5 never made any extortion payments to DARDAR.

V. VICTIM 6, an Online Entertainment Service, Is Extorted

49. In or about May 2014, DARDAR successfully compromised computer systems belonging to an online entertainment service that has offices in the United States and elsewhere (VICTIM 6). Specifically, on or about May 21, 2014, VICTIM 6 employees received spearphishing emails that appeared to be from its CEO with a purported hyperlink to a news article regarding VICTIM 6, but which instead directed recipients to a Conspiracy-controlled

website that mimicked the log-in portal for VICTIM 6's email system. At least one recipient clicked on the embedded hyperlink and, when prompted by the fake log-in portal, entered valid credentials. DARDAR subsequently started receiving emails in his ethicalspectrum@gmail.com account that contained what appeared to be credentials for VICTIM 6 employees, thereby indicating that some VICTIM 6 employees had clicked on the hyperlink and been deceived into entering their credentials. DARDAR used the information to change the settings of the affected accounts in order to divert some employees' emails to the email account arsenlopen1989@googlemail.com.[7] For example, DARDAR received an email containing the login information for one VICTIM 6 employee; four minutes later he received an email from VICTIM 6's email service provider indicating that the purported employee had requested to automatically forward email to arsenlopen1989@googlemail.com. According to interviews of VICTIM 6 employees, valuable data was exfiltrated from VICTIM 6's servers as a result of the intrusion.

50. Later that day, DARDAR, using the ethicalspectrum@gmail.com account, sent the following message to several VICTIM 6 employees:

> Hello [VICTIM 6]
> I'm an ethical hacker i worked for many big and small companies
> i hacked all your server and maybe i hacked your databases too
> i can help you to avoid this hack again but i want fees in return
> you can see in this articles the last companies that didn't even respond at my email
> NOTE:

[7] The investigation has revealed that DARDAR controlled the arsenlopen1989@googlemail.com account. Specifically, a court-authorized search of the account revealed that on or about May 23, 2013, the email account received an automated email from Apple, Inc. (Apple). The email was addressed to "SEA Shadow" and indicated that the account was linked to an Apple account. Subscriber records provided by Apple indicated that the account was registered to DARDAR ("fares derar").

> this is only the companies that didn't respond at my emails , as i said before i worked for a lot of companies
> . . .
> [Internet links to articles regarding computer intrusions conducted by "Ethical Spectrum," including the hack into VICTIM 5's systems.]
> . . .
> so are you interested in this deal or not ?
> DON'T IGNORE THIS EMAIL
> you must to respond at least with YES or NO
> I repeat
> (((((DON'T IGNORE THIS EMAIL))))))

The next day, after no one responded, DARDAR sent another series of emails stating, "you may think this is a joke / you have 20 min to respond."

51. Subsequent correspondence between representatives of VICTIM 6 and DARDAR indicate that representatives of VICTIM 6 eventually responded to DARDAR's threatening emails and, after DARDAR provided proof that he had accessed VICTIM 6's databases, representatives of VICTIM 6 agreed to pay DARDAR €7,500 in exchange for information on how DARDAR perpetrated the attack. As part of the negotiations over the price, Dardar sent the following message (emphasis added):

> so i think you are agree on 7500 EUR
> ok then you must to know that i'm from Syria
> and
> you should have to send money outside the U.S.
> *Because U.S. does not deal with the Syrian banks because of USA sanctions*
> I suggested to send money from China, Britain, Russia or Germany

52. Over the next few days, DARDAR and several VICTIM 6 employees exchanged multiple emails regarding payment to Syria. In one email dated on or about May 26, 2014, DARDAR indicated that if there was a problem transferring money to Syria, then VICTIM 6 could send the money to ROMAR in Germany. DARDAR attached a photograph of the back of ROMAR's bank card, which included information regarding ROMAR's account.

53. Subsequent email correspondence reveals that VICTIM 6 refused to pay DARDAR because doing so would violate U.S. sanctions against Syria. DARDAR responded by issuing further threats against VICTIM 6, including: "[W]hat do you expect me to do now[?] [smiley face] [D]o you know what I have [--] info about your company?"

54. VICTIM 6 never paid DARDAR, according to a representative from the company.

VI. VICTIM 7, a Swiss Web Hosting Provider, Is Extorted

55. In or around July 2014, DARDAR obtained unauthorized access to the computer servers of a Switzerland-based web hosting service (VICTIM 7). On or about July 26, 2014, DARDAR sent an email from his codezero70@gmail.com account to several VICTIM 7 employees containing what appeared to be an employee's username and password as proof of the infiltration, and indicated that "I can help you to avoid this hack again but I want fees in return."

56. The next day, on or about July 27, 2014, DARDAR and representatives of VICTIM 7 negotiated over email a price of €5,000 in exchange for a report on how DARDAR perpetrated the attack. DARDAR instructed VICTIM 7 to send the money to ROMAR's PayPal account and described ROMAR as "my partner and he [is] responsible for receiving money and sent me only [sic]." On or about July 27, 2014, VICTIM 7 sent DARDAR an email with an attached scan of a statement indicating that it was sending money to ROMAR's PayPal account in exchange for "ethical penetration testing received." Based on my training and experience, and my familiarity with this investigation, I believe that DARDAR would, in some instances, include such statements in his "contracts" (or ask that the victim include them) in order to provide his extortionate activities with a false veneer of legitimacy. DARDAR forwarded the agreement to ROMAR by email.

57. On or about July 28, 2014, ROMAR received emails from PayPal indicating that three payments totaling €5,000 had arrived from a Swiss bank account. ROMAR forwarded at least one of those emails to DARDAR's sea.the.shadow@gmail.com account. DARDAR thereafter informed representatives of VICTIM 7 that he had received the funds, thereby confirming that these payments were from VICTIM 7.

58. According to emails ROMAR received from PayPal and Romar's personal bank records, ROMAR transferred the funds (minus apparent small administrative fees) from his PayPal account to his bank account with Sparda-Bank Berlin on or about July 31, 2014.

CONCLUSION

59. Based on the forgoing, I request the Court issue the attached complaint and arrest warrants.

Respectfully submitted,

Patrick DiMauro
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on September 29, 2015:

/s/
Michael S. Nachmanoff
United States Magistrate Judge

HON. MICHAEL S. NACHMANOFF
UNITED STATES MAGISTRATE JUDGE

Submitted by AUSAs Maya D. Song and Jay V. Prabhu