AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A Computer Accessing E-mail Account
lavandos@dr.com

Case No. MJ-16-551

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington or elsewhere, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 875 (d)	Interstate Threats to Extort
18 U.S.C. § 1030 (a)(5)	Damaging to a Protected Computer
18 U.S.C. § 1030 (a)(7)	Extortion by Threatening or in Relation to Damaging a Protected Computer

The application is based on these facts:

See Affidavit of Chris Hansen, Seattle Police Department, United States Secret Service Task Force Officer, which is attached hereto and incorporated herein by reference

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of _____ days (give exact ending date if more than 30 days: 04/23/2018) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Chris Hansen, SPD-USSS Task Force Officer
Printed name and title

Sworn to before me pursuant to CrimRule 4.1.

Date: Dec 23, 2016

Judge's signature

City and state: Seattle, Washington

James P. Donohue, United States Magistrate Judge
Printed name and title

USAO #2016R01459

ATTACHMENT A

Location to be Searched

This warrant authorizes the use of a network investigative technique on any computer accessing the e-mail account lavandos@dr.com.

ATTACHMENT B

Information to be Seized

The following information that may assist in identifying the computer, its location, other information about the computer, and the user of the computer, all of which is evidence of violations of 18 USC §§ 875(d), 1030(a)(5), and 1030(a)(7)(A) & (C):

a. The computer's IP address and the communication port number used by the computer to access the United States Secret Service server.

b. The computer's open communication ports.

c. The type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 10), and license number.

d. The computer's language encoding and default language.

e. The computer's time zone information.

f. The registered computer name (more commonly referred to as the "host name") and registered company domain name.

g. The user name of the currently logged-in user.

h. A list of the user names of other local user accounts on the computer.

i. The computer's wired and wireless network connection information.

j. A list of the wireless network identifiers of wireless access points that have been saved to the computer.

k. The list of IP addresses and port numbers of currently-connected and recently-connected computers.

AFFIDAVIT

I, Chris Hansen, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am an officer with the Seattle Police Department (SPD), commissioned through the Washington State Criminal Justice Training Commission, and have been since June 2000. I received my law enforcement training from the Washington State Criminal Justice Training Commission Basic Law Enforcement Academy. I serve as a Detective in SPD's Fraud, Forgery and Financial Exploitation Unit. In that capacity, I have conducted investigations involving forgery, theft, possession of stolen property, credit card fraud, Internet fraud, embezzlement, securities fraud, insurance fraud and identity theft.

2. I currently serve as a computer forensic examiner and task force officer on the United States Secret Service - Electronic Crimes Task Force (USSS-ECTF), and, in connection with that assignment, have been specially deputized as a Special Deputy United States Marshal. I have served as a task force officer for the USSS-ECTF since August 2008, and as a computer forensic examiner since March 2010. During the course of this assignment, I have participated in investigations of numerous electronic crime cases, including network intrusion incidents, point-of-sale breach incidents, skimming incidents, sales of credit card dumps, e-mail phishing schemes and credit card cashout schemes. During my time on the USSS-ECTF, I have received over 1,400 hours of training in digital forensics, including courses on the topics of network intrusion and point-of-sale breach investigations.

3. I make this affidavit in support of applications under Rule 41(b)(6)(A) of the Federal Rules of Criminal Procedure for two search warrants to use network investigative techniques (NITs). One of those two applications requests approval to send communications to the e-mail account lavandos@dr.com that are designed to cause

whatever computer is used to open these communications to transmit data that will identify the computer, its location, other information about the computer, and the user of the computer. The other application requests approval to send communications to e-mail account lavandos@india.com that are designed to cause whatever computer is used to open these communications to transmit the same data concerning that computer.

4. As set forth herein, there is probable cause to believe that the user(s) of the e-mail accounts lavandos@dr.com and lavandos@india.com have committed violations of 18 U.S.C. § 875(d) (which prohibits transmission in interstate and foreign commerce of threats to injure property that are made with the intent to extort), 18 USC § 1030(a)(5) (which prohibits transmitting programs, code, and commands to protected computers and, thereby, damaging such computers), and 18 USC § 1030(a)(7)(A) & (C) (which prohibit threatening to damage a protected computer and demanding money in relation to damaging a protected computer). There also is probable cause to believe that evidence of the identity of the person(s) who have committed these violations exists on the computers that will be used to open communications sent to these two e-mail accounts, and that this evidence will be obtained through the use of the NITs for which this Affidavit is being submitted.

5. This information contained in this Affidavit is based on my own investigation, as well as upon information received from the persons identified in this Affidavit. This Affidavit does not contain all of the information that I have gathered during my investigation. Rather, the Affidavit contains only the information that I believe is relevant to the determination of probable cause for the requested warrants.

THE INVESTIGATION

6. On December 6, 2016, the USSS Seattle Field Office received a request for assistance from a representative of the South Correctional Entity (SCORE) Jail in Des Moines. The SCORE Jail is a jail in Des Moines, Washington, that serves seven member cities and a number of contract agencies. The SCORE Jail reported that it had just

discovered ransomware on its computer network. I subsequently participated in a telephone call with A.M, the Information Technology Director for the SCORE Jail.

7. A.M. told me that a user on the SCORE Jail's computer network had reported that the user was unable to access the user's computer files on a server that the SCORE Jail uses to facilitate remote searches of jail records by law enforcement officers with accounts on the SCORE Jail computer system. That server is accessible through the world wide web, and when users (even those in Washington State) contact it, their communications commonly are routed through other states. According to A.M., the files all had been renamed by the addition of the extension ".[lavandos@dr.com].wallet" to the files' names, and the files no longer could be opened by the computer programs that previously had been used to create and access the files.

8. In addition to the now-inaccessible files, A.M. located a JPG computer file on the SCORE Jail's computer system that contained the following text:

> //hallo, our dear friend! //looks like you have some troubles with your security //all your files are now encrypted //using third-party recovering software will corrupt your data //you have only one way to get them back safely – using our decryption tool //to get original decryption tool contact us with email in subject line write your ID, which you can find in name of every crypted file, also attach to email 3 crypted files lavandos@dr.com //it is in your interest to respond [sic] as soon as possible to ensure the restoration of your files, because we won't keep your decryption keys at our servers more than 72 hours in interest of our security //P.S. only in case you don't receive a response from the first email address within 24 hours, please use this alternative email address lavandos@india.com.

Based upon my experience and training, I believe that the person(s) who encrypted SCORE Jail files, and sent this message to the SCORE Jail, is/are perpetrating a "ransomware" scheme – that is, a scheme in which a victim's computer files are held hostage through encryption, and in which the perpetrator(s) will demand payment in order to decrypt the files.

9. According to Whois.com, a website that provides information concerning web domains, the domains dr.com and india.com both are registered to World Media Group, LLC, a Bedminster, New Jersey, company. I do not have any additional information identifying the person or entity who established the specific e-mail addresses lavandos@dr.com and lavandos@india.com.

10. A.M. further stated the malware accessed the system through the account of a user with the user name vmartinez, who, an Auburn, Washington, police officer. The SCORE Jail believes that vmartinez is himself a hacking victim, rather than the perpetrator of the ransomware scheme I am investigating. A.M. also stated that the vmartinez account on the SCORE jail computer system had been accessed from a number of different Internet Protocol addresses (IP addresses) at different locations over a period of months.

11. While we were speaking, A.M. noticed an unfamiliar program named bendix.exe running in the Downloads folder for the vmartinez user account. A.M. made a copy of bendix.exe. I asked A.M. to make an image of the RAM on the machine on which bendix.exe was currently running. A.M. began to collect the RAM image while we continued to speak. A short time later, A.M. reported that the malware was now encrypting and renaming files in the computer folder to which the RAM capture was being saved.

12. On December 9, 2016, at my direction, A.M. sent an e-mail to the e-mail address lavandos@dr.com that stated, "Please help. I don't understand your instructions to get my files back. You say there is an ID, what does it look like. Is it a number? What do you need me to do? I need to get my files back ASAP. \\[A.M.], Information Technology Director." Shortly after sending that e-mail, A.M. received an e-mail from lavandos@dr.com that stated, "hello, [A.] \\just send us 3 crypted files \\after this i will tell you how to proceed." I inspected the e-mail header information and observed the originating IP address address was 37.220.35.202. I checked the IP address via

domaintools.com and discovered that this IP address was listed as a Tor exit node operated by Rens Ariens of YISP Colo in the Netherlands.

13. The Tor network is a publicly-available tool used for anonymizing a user's web traffic. It is a network that provides free access to all subscribers. The network obfuscates a user's location by encrypting the user's connection and routing the user's traffic through multiple participating nodes to complete an anonymous connection. As a result, the fact that the e-mail emanated from a Tor exit node in the Netherlands does not actually indicate that the sender of the e-mail is in the Netherlands. Rather, it is impossible to determine the sender's location.

14. According to A.M., the ransomware attack on the SCORE Jail's file servers caused a major disruption to work for over 12 hours. The ransomware infected a primary network share used by every employee at the SCORE Jail that contains files essential for their job duties. Once discovered, the network share had to be taken offline to stop further infections. SCORE Jail had to restore the contents of the shared folder from the previous night's off-site backup, which caused a loss of data from any file modifications made in the interim. The ransomware also infected a software program used by several law enforcement agencies to create lineup montages, infecting the image files used for creating these lineups and preventing law enforcement officers from accessing the system to look up inmate booking photos and tattoo images.

PLACES TO BE SEARCHED AND PROPERTY TO BE SEIZED

15. Based on my training, experience, and the information described above, I believe that using a NIT may help identify the user(s) of the lavandos@dr.com and lavandos@india.com e-mail accounts. Accordingly, this warrant application seeks authority to use the NIT, which will be deployed via e-mail to these two e-mail accounts.

16. Specifically, the NIT will cause a computer on which it is opened to send various identifying information regarding that computer back to a computer controlled by the USSS. I intend to conceal the NIT within a file named Shift Scheduler Installer. I then intend to zip (that is, compress) the file. With the cooperation of the SCORE Jail, I

intend to then place the zipped file on the SCORE Jail's computer and to expose it to the malware on the SCORE Jail's system. Exposing the zipped file to the malware will cause the zipped file to become encrypted.

17. Once the malware has encrypted the zipped file containing the NIT, the SCORE Jail will send this encrypted file, and two other encrypted files, to lavandos@dr.com and, subsequently, to lavandos@india.com. I expect that, when the perpetrator(s) of the ransomware scheme receive(s) these encrypted files, the perpetrator(s) will use an encryption key to unencrypt the files and will then return the unencrypted files to the SCORE Jail as proof that the perpetrator(s) of the ransomware scheme are able to decrypt encrypted files.

18. At that point, the SCORE Jail will contact the perpetrator(s) of the ransomware scheme and tell the perpetrator(s) that the unzipped Shift Scheduler Installer file is not functional. The SCORE Jail will ask the perpetrator(s) to examine the unzipped file and to repair it. The SCORE Jail also will e-mail the perpetrator(s) a copy of the unencrypted file (to cover the possibility that the perpetrator(s) did not retain a copy of the file). If the perpetrator(s), in fact, examine(s) the unzipped file, and in doing so attempt(s) to run the file, the action of pressing the "run" button will launch the NIT.

19. Once activated, the NIT will conduct a one-time limited search of the computer on which the NIT has been launched. Specifically, the NIT will collect information that will assist in identifying the computer, its location, other information about the computer, and the user of the computer. The NIT will then cause this information to be sent over the Internet to a computer controlled by the USSS. The information that the NIT will collect and send to the USSS is:

a. The computer's IP address and the communication port number used by the computer to access the USSS server. An IP address is a unique numeric address used to direct information over the Internet. An IP version 4 (IPv4) address is a 32-bit binary number (a

sequence of 32 ones and zeros representing a number to a computer). For convenience of reading and writing by humans, IPv4 addresses are typically represented by four decimal numbers in the range 0-255, separated by periods (e.g., 121.56.97.178). An IP version 6 (IPv6) address is a 128-bit binary number (a sequence of 128 ones and zeros representing a number to a computer). For convenience, an IPv6 address is typically written as eight groups of four hexadecimal digits (using the characters 0-9 and A-F), separated by the colon character (e.g., 2001:0db8:0000:0042:0000:8a2e). Conceptually, IP addresses are similar to telephone numbers in that they are used to identify computers that send and receive information over the Internet. A communications port number is used in different ways by a "server" computer (a computer that is "listening" for incoming connections) and a "client" computer (a computer that initiates a connection to a server computer). A server computer "listens" on one or more standard communications ports that are associated with particular services. For example, a web server is expected to listen on port 80 for connections to serve web pages. A client computer uses a communications port number as an identifier to receive return information coming back from a server, and to keep concurrent connections with different servers separated. Conceptually, a port number is like a

telephone extension number at an office with multiple phones served by the same telephone number. The standard port numbers such as 80 for a web server are analogous to published extensions at a business, such as extension 0 for the operator. The port number used by the client is analogous to a telephone number and extension that a caller records in a voicemail message to allow the business to call the client back.

b. The computer's open communication ports.

c. The type of operating system running on the computer, including type (e.g. Windows), version (e.g. Windows 10), and license number.

d. The computer's language encoding and default language. Users can set computers to display text in a particular language.

e. The computer's time zone information.

f. The registered computer name (more commonly referred to as the "host name") and registered company domain name. Users can input this information when the computer's operating system is first installed and may update this information later.

g. The user name of the currently logged-in user account.

h. A list of the user names of other local user accounts on the computer.

i. The computer's wired and wireless network connection configuration information. This information identifies the way the computer is connected to the Internet.

j. A list of the wireless network identifiers of wireless access points that have been saved to the computer. This list identifies wireless networks that the computer previously connected to and which were saved by operator of the computer. This may identify other ways that the computer connects to the Internet.

k. The list of IP addresses and port numbers of currently-connected and recently-connected computers. This list identifies other computers that the computer is connected to or has recently connected to, and may identify whether the operator of the computer has connected to it remotely from another computer.

20. Each of these categories of information can help to identify the computer receiving the NIT and/or that computer's user. The computer's true assigned IP address can be associated with an Internet Service Provider ("ISP"), and through that, a particular ISP customer. The communications port number being used to communicate to the USSS server is required by some ISP companies along with the IP address and the date and time of communication to particularly identify a customer. This is typically required in those cases where an ISP with many customers but few assigned IP addresses uses the same IP address (but different port numbers) for several customers, and keeps records about which customer was assigned each port number. The operating system can corroborate the identity of a computer and, in the case of an operating system's license number, identify the user, because some companies maintain records of purchasers of their operating systems. The language encoding and computer default language can help identify the subject by identifying his native language. Time zone information can establish the geographical location of the subject computer. The computer name, company name, logged-in user name, and list of user names of other user accounts can identify the network, specific computer on a network, and perhaps even the name of the

person using the computer. Wireless network connection information can tell from where a computer accessed the Internet, even if it was through the unauthorized use of a wireless network (a technique used by Internet criminals). Wired network information and dial-up account information can help identify what computer was used to access the Internet to receive the NIT. The list of open and recent connections may reveal the IP address used by the subject to connect remotely from another computer to the computer on which the subject actually opens e-mails and launches the NIT.

21. I believe that using a NIT is necessary in this case, because the perpetrator(s) of the ransomware scheme have used the Tor network to conceal the IP address from which the perpetrator(s) is/are communicating with the SCORE Jail. The information provided by the NIT should help identify the perpetrator(s) of the scheme, despite this deliberate concealment.

22. Because the NIT will be delivered by e-mail addressed to the e-mail accounts lavandos@dr.com and lavandos@india.com, and because it is being delivered in an encrypted file, the NIT can be accessed only by someone who has access to one of these e-mail accounts, and who also has access to the decryption keys for the ransomware scheme that I am investigating. As a result, the NIT will only search, and identify, a computer being used by a perpetrator of the scheme, as opposed to any other computer.

TIME AND MANNER OF EXECUTION OF THE SEARCH

23. Rule 41(e)(2) of the Federal Rules of Criminal Procedure requires that a warrant command the law enforcement officer (a) "to execute the warrant within a specified time no longer than 14 days" and (b) to "execute the warrant during the daytime unless the judge for good cause expressly authorizes execution at another time . . . ." I hereby request permission to deploy the NIT at any time of day or night within 14 days of the date the warrants are authorized. There is good cause to allow such a method of execution, since the time of deployment causes no additional intrusiveness or inconvenience to anyone. In addition, the government will not be able to control the time when a subject accesses the lavandos@dr.com and lavandos@india.com e-mail accounts

and when the subject seeks to run the unencrypted Shift Scheduler Installer software, and thereby launches the NIT.

DELAYED NOTIFICATION

24. I hereby request that the Court authorize me to delay notification of the execution of the warrant for a period of 180 days after the execution of the warrant. 18 U.S.C. § 3103a(b) authorizes delayed notification where certain conditions are met. Those conditions are met in this case because:

a. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. The perpetrator(s) of the ransomware scheme is/are not aware that I am seeking to use a NIT to identify and locate their computers, and, through that, the perpetrator(s). Providing immediate notice to perpetrator(s) of the scheme would seriously jeopardize the ongoing investigation, since such a disclosure would give the perpetrator(s) an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. See 18 U.S.C. § 2705.

b. The warrant does not seek the seizure of any tangible property, or any wire or electronic communication. To the extent the warrant authorizes the seizure of stored wire or electronic information, there is a reasonable necessity for its seizure, since the information to be seized is limited in scope and necessary to identify the perpetrators of the ransomware scheme.

c. This investigation is likely to take a substantial time. Even if the NIT succeeds, the information obtained through the use of the NIT may provide leads, but not fully identify the perpetrator(s) of the ransomware scheme. Additional investigation to complete that identification, and gather necessary electronic evidence before it is destroyed is likely to take many months. As a result, a one-year delay in notification is reasonable. (In the event that the investigation is completed more quickly, and the perpetrator(s) arrested in less than 180 days, I will provide notification promptly following the arrest.)

JURISDICTION

25. This Court has jurisdiction to issue the requested warrant under recently-amended Rule 41(b)(6)(A), even if the computers to be searched are outside this District, because the above facts establish there is probable cause to believe that the location of the computers accessing the e-mail accounts being used by the perpetrator(s) has been concealed through technological means, namely, the use of the Tor network, and that there is probable cause to believe that activities related to the crime being investigated, namely, the hacking of the SCORE Jail's computers, have occurred within this judicial district.

REQUEST FOR SEALING

26. I further requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing these document is necessary because the search is part of an ongoing investigation. Based upon my training and experience, I have learned that online criminals commonly search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate,

e.g., post them publicly online through the criminal forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation, including by allowing perpetrator(s) an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution.

CONCLUSION

27. Based on the information identified above there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 875(d), 1030(a)(5) and 1030(a)(7)(A) & (C) will be found on the computer(s) that access the e-mail accounts lavandos@dr.com and/or lavandos@india.com and to believe that employing the NIT sought by this affidavit will result in the seizure of that evidence.

CHRIS HANSEN
Detective, Seattle Police Department
TFO, United States Secret Service

AFFIDAVIT subscribed and sworn to before me this 23rd ~~th~~ day of December 2016

JAMES P. DONOHUE
United States Magistrate Judge

Approved as to form:

ANDREW C. FRIEDMAN
Assistant United States Attorney