

United States District Court
for the
Western District of New York

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address.)

THE USE OF A NETWORK INVESTIGATIVE TECHNIQUE FOR A
COMPUTER ACCESSING EMAIL ACCOUNT:
PERSONNEL@MANAGEMENTS-SECUREMAILS-OFFICE-PORTALS.COM

Case No. 17-MJ- 627

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)*: **THE USE OF A NETWORK INVESTIGATIVE TECHNIQUE FOR A COMPUTER ACCESSING EMAIL ACCOUNT: PERSONNEL@MANAGEMENTS-SECUREMAILS-OFFICE-PORTALS.COM**, as more particularly described in Attachment A,

located in the Western District of New York, there is now concealed *(identify the person or describe the property to be seized)*: **See Attachment B for the Items to be Seized, all of which are fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 1028A; Title 18, United States Code, Section 1341; Title 18, United States Code, Section 1343; and Title 18, United States Code, Section 1349, and all of which are more fully described in the application and affidavit filed in support of this warrant, the allegations of which are adopted and incorporated by reference as if fully set forth herein.**

The basis for 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 **Title 18, United States Code, Section 1028A; Title 18, United States Code, Section 1341; Title 18, United States Code, Section 1343; and Title 18, United States Code, Section 1349.**

The application is based on these facts:

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

Applicant's signature

Meredith McClatchy, Special Agent
Federal Bureau of Investigation

Printed name and title

Sworn to before me and signed in my presence.

Date: July 31 2017

Judge's signature

HONORABLE JONATHAN W. FELDMAN
UNITED STATES MAGISTRATE JUDGE

Printed name and Title

City and state: Rochester, New York

ATTACHMENT A

Location to be Searched

This warrant authorizes the use of a network investigative technique on the portion of any computer accessing TARGET EMAIL that may assist in identifying the computer, its location, other information about the computer, and the user of the computer.

ATTACHMENT B

Information to be Seized

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, instrumentalities, contraband and fruits of violations of Title 18, United States Code, Sections 1028A (Aggravated Identity Theft), 1341 (Frauds and Swindles), 1343 (Wire Fraud), and 1349 (Attempts and Conspiracy). This information may include environmental variables and/or certain registry-type information, such as:

1. The computer's IP address.
2. The computer's User Agent String.

This warrant does not authorize the physical seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of stored wire and electronic information as described above. See 18 U.S.C. § 3103a(b)(2).

This warrant authorizes the subsequent surreptitious removal of the code used to execute this warrant and evidence of the code or remote access without notice, and without further authorization being required. Provided, however, that all information will be extracted from the target computer during the time period authorized for the execution of this warrant.

In light of the unique search procedures authorized by this warrant, the government shall provide a progress report to the Court as to the identification of the computer accessing the email accounts particularized in this warrant once any of the operations set forth in paragraphs 39, 43 and 44 of the search warrant application have been deployed or accessed by the "target user."

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF:
THE USE OF A NETWORK
INVESTIGATIVE TECHNIQUE FOR A
COMPUTER ACCESSING EMAIL
ACCOUNT
PERSONNEL@MANAGEMENTS-
SECUREMAILS-OFFICE-
PORTALS.COM

Case No. 17-MJ- 627

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Meredith McClatchy, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent with the Federal Bureau of Investigation (FBI) since June, 2017. I am currently assigned to the Cyber Squad, Buffalo Division, in Rochester, New York. As part of the Cyber Squad, I work on investigations relating to criminal and national security cyber intrusions. I have gained experience through training and everyday work related to these types of investigations. I am familiar with fundamental operations of the internet, hardware, software, and the communication protocols across each. Experience with similar investigations and working with other FBI Special Agents and computer forensic professionals has expanded my knowledge of internet communications and, more specifically, internet based obfuscation techniques. I have participated in the execution of warrants involving the search and seizure of computers, computer equipment, mobile phones

and tablets, and electronically stored information, in conjunction with various criminal investigations.

2. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

3. I make this affidavit in support of an application under Rule 41(b)(6)(A) of the Federal Rules of Criminal Procedure in support of an application for a search warrant to use a network investigative technique (“NIT”). I request approval to send one or more communications to any computer accessing personnel@managements-securemails-office-portals.com (TARGET EMAIL). Each such communication is designed to cause the computer receiving it to transmit data that will help identify the computer, its location, other information about the computer, and the user of the computer. As set forth herein, there is probable cause to believe that violations of Title 18, United States Code, Section 1028A (which makes it a crime to knowingly transfer, possess, or use, without lawful authority, a means of identity of another person during and in relation to any felony); Title 18, United States Code, Section 1341 (which makes it a crime to use a mail carrier in furtherance of a Scheme or Artifice to defraud for money or property by means of false pretenses, representations, or promises); Title 18, United States Code, Section 1343 (which makes it a crime to devise a scheme for obtaining money by means of fraudulent pretenses and then transmit or cause to be transmitted by means of wire in interstate or foreign commerce, any

writings for the purpose of executing such scheme); and Title 18, United States Code, Section 1349 (which makes it a crime for two or more persons to commit offense of Mail, Bank, or Wire Fraud) (the TARGET OFFENSES) have occurred and that evidence, instrumentalities, contraband and fruits of those violations exist on the computer that receives the NIT described above.

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

RELEVANT STATUTES

5. This investigation concerns alleged violations of: 18 U.S.C. § 1028A – Aggravated Identity Theft, 18 U.S.C. § 1341 – Frauds and Swindles, 18 U.S.C. § 1343 –Wire Fraud, and 18 U.S.C. § 1349 – Attempts and Conspiracy.

- a. 18 U.S.C. § 1028A prohibits a person from, during and in relation to any felony violation of mail, bank, or wire fraud, knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person.
- b. 18 U.S.C. § 1341 prohibits a person from devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, or to sell, dispose of, loan, exchange, alter, give away, distribute, supply, or furnish or procure for unlawful use any counterfeit or spurious coin, obligation, security, or other article, or anything represented to be or intimated or held out to be such counterfeit or spurious article, for the purpose of executing such scheme or artifice or attempting so to do, places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service.
- c. 18 U.S.C. § 1343 prohibits a person from devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any

writings, signs, signals, pictures, or sounds for the purpose of executing such scheme.

- d. 18 U.S.C. § 1349 prohibits a person from attempting or conspiring to committing 18 U.S.C. § 1343 or 18 U.S.C. § 1341.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

6. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”

7. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

8. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work.

Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

9. “Computer passwords, pass-phrases and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

10. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

11. “Attachment” refers to a data file (examples include Microsoft Word, PDF, or picture file) that, when included with an email, transfers the file directly to the recipient(s) of the email.

12. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between

devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

13. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (“DSL”) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

14. “Internet Protocol address” or “IP address” is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots, e.g., 149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic, sent from and directed to that

computer, is directed properly from its source to its destination. Internet Service Providers (ISPs) assign IP addresses to their customers' computers.

15. "Proxy Server" or "Proxy" is a computer that acts as a gateway between a local network (e.g. all of the computers at one company or building) and a larger-scale network such as the internet. A Proxy Server can be used to protect a users' privacy by routing a user's IP Address through an intermediary computer, thereby masking the user's actual IP address and location which could otherwise be used to identify a user. It prevents someone attempting to monitor an Internet connection from learning what sites a user visits, prevents the sites the user visits from learning the user's physical location, and it lets the user access sites which could otherwise be blocked. Because of the way proxy services route communications through other computers, traditional IP identification techniques are not viable. When a user using a proxy service accesses a website, for example, the IP address of the proxy service, rather than the user's actual IP address, shows up in the website's IP log.

16. "Virtual Private Network" or "VPN" is a digital network that connects to a private network over the internet. It allows remote computers to act as though they were on the same secure, local network, emulating the properties of a point to point private link. For example, someone working from home on their home network can connect to their company's network though a VPN. When a user accesses a website or data though a VPN, it would show the IP Address of the VPN server the user connected to the website through, not their true IP Address. When connecting to the internet through a VPN service, a user has the ability to choose the country and city they would like to appear to be from, which can obfuscate their geographic location.

PROBABLE CAUSE

17. Gorbel, Inc. is a cranes, ergonomic lifting, and fall protection products manufacturing company headquartered in Fishers, New York. They also have a manufacturing facility in Pell City, Alabama, and a sales and manufacturing facility in Tianjin, China.

18. On June 21, 2017, Gorbel, Inc. received an email from the address executive.office@management-securemailservers-office-portal.online. The cyber actor sending the email portrayed themselves to be the CEO of Gorbel, Inc., Brian Reh, and emailed a member on the Accounts Payable team, Margaret Belt. The actor asked "Margaret, Can we set up a payment to a new vendor today? Thanks, Brian". Belt responded to the fraudulent email saying that they could do that and needed all the appropriate information. The cyber actor responded "Margaret, See attached W9 and invoice for vendor details, Please have check made out to "LCAP HOLDINGS LLC" for \$82,570.00 and have it sent by overnight mail. Payment is for professional service, Charge this to Admin Dept and email me with tracking# once check is mailed out. Thanks, Brian". The attached W-9 provided the following information for the check recipient: Lynn Palmer, LCAP HOLDINGS LLC, Social Security Number 201-46-2829, 20 N 100W Tremonton, UT 84337.

19. Belt mailed a cashier's check issued by Key Bank in Rochester, New York for \$82,570.00 paid to the order of LCAP HOLDINGS LLC to 20 N 100W Tremonton, UT

84337 on June 21, 2017. The FedEx Tracking slip #811745126923 shows that the package was received on June 22, 2017 and signed for by "L. Palmer".

20. On July 14, 2017, Relationship Manager Sheila Hanley of Key Bank indicated that the check had been cashed out at Mountain West Bank on June 27, 2017. Mountain West Bank is headquartered in Coeur D Alene, Idaho, and has locations throughout Idaho, Utah, Montana, and Washington.

21. A financial analyst at Gorbel inquired about the payment to LCAP HOLDINGS, LLC. during an audit of financial transactions for the month of June. Gorbel, Inc., Chief Financial Officer, Gay Card, reviewed all records relevant to the payment to LCAP HOLDINGS, LLC. and identified that a fraudulent transaction took place due to the numerous irregularities. Card contacted FBI Buffalo, Rochester Resident Agency regarding the fraudulent transaction on July 14, 2017. Your affiant interviewed Card, Reh, and a Gorbel, Inc. Computer Operations Manager on July 17, 2017 during which time all emails with the fraudulent actor and supporting documentation of the payment to LCAP HOLDINGS, LLC. were voluntarily provided to the FBI. The investigation determined that the email executive.office@management-securemailservers-office-portal.onlie was an email address hosted by Google, Inc.

22. On July 18, 2017, Belt received emails from personal@office-portal-server-secure.management and personal@managements-securemail-office-portal.com, both of which saying "Margaret, Can we set up payment to a new vendor today? Brian". Your affiant determined that both of the email addresses were hosted by Google, Inc.

23. On July 19, Belt emailed personal@managements-securemail-office-portal.com and personal@office-portal-server-secure.management saying she could set up a payment to the new vendor but needed all of the appropriate information. This was done in an attempt to gain further subject identifiers. On July 22, 2017, Belt received a reply from mailer-daemon@googlemail.com indicating that the email address personnel@managements-securemail-office-portal.com had been disabled. Belt never received a response back from the email address personal@office-portal-server-secure.management. Based on the automated response from Google, your Affiant believes that on or before July 22, 2017, the email account personnel@managements-securemail-office-portal.com had been disabled and was no longer in use by the cyber actor.

24. On July 19, 2017, Gorbel, Inc. received an email from the address personnel@managements-securemails-office-portals.com (note the minor change in previous email addresses used). The cyber actor again portrayed themselves to be the CEO of Gorbel, Inc. and again emailed Belt. The actor asked "Margaret, Can we set up a payment to a new vendor today? Thanks, Brian". Belt, knowing the email was fraudulent, responded to the email saying that they could do that and needed all the appropriate information. The cyber actor responded "Margaret, See attached W9 for vendor details, Please have check made out to "[a person with the initials J.C.Q.]" for \$138,580.00 and have it sent by overnight mail. Payment is for professional service, Charge this to Admin Dept and email me with tracking# once check is mailed out. Thanks, Brian". The attached W-9 provided the following

information for the check recipient: J.Q., Social Security Number XXX-XX-2821, 1310 Louisville Rd. #XX, Frankfort, KY 40601.

25. On July 20, 2017, the cyber actor emailed Margaret Belt asking “Margaret, Has the payment been processed? Thanks, Brian”.

26. On July 21, 2017, the cyber actor emailed Margaret Belt again asking “Margaret, I got no response from you, Has payment been mailed out? Brian”.

27. On July 21, 2017, Belt emailed back the cyber actor using a ruse to keep them engaged. Belt told the cyber actor that Gorbels check printer was broken and the check would be mailed when the machine was fixed. On July 21, 2017, the actor emailed Ms. Belt back the same day saying “Payment is already due, Let me know once mailed out on Monday”. On July 24, 2017, Ms. Belt emailed back the actor continuing the ruse, saying that during the repair of the printer it was discovered that a new part needed to be ordered and there would be further delay on delivering the check. On July 25, 2017, the actor responded to Ms. Belt asking to be notified when the check went out. On July 26, 2017, the actor emailed Ms. Belt “Margaret, Do you have an update regarding payment? I believe the printer should be fixed by now. Please advise. Brian”.

28. On July 25, 2017, FBI Buffalo, Rochester Resident Agency purchased the domain www.fedextrackingportal.com and developed the website www.fedextrackingportal.com/apps/us-en/tracking.php?action=track&trackingnumber=731246AF7684.

The website was created with the message “Access Denied, This website does not allow proxy connections” error message when accessed. The website was created to capture the basic server communication information, as IP Address date and time stamp, and user string when the website was accessed. No malware or computer exploit was deployed in the development of the website; the only information captured in the webserver logs was unencrypted basic network traffic data identified above.

29. On July 26, 2017, Belt, in coordination with FBI Buffalo / Rochester Resident Agency, emailed the cyber actor saying that they payment (check) was made yesterday and provided the hyperlink www.fedextrackingportal.com/apps/us-en/tracking.php?action=track&trackingnumber=731246AF7684.

30. On July 26, 2017 the actor accessed the FBI operated website from IP Address 173.239.197.74 at 2:42:43PM EST, 2:42:44 PM EST, and 2:44:38 PM EST. Open source searches of IP Address 173.239.197.74 identified it is assigned to ExpressVPN, a domestic Virtual Private Network provider. The actor accessed the website again from IP Address 212.83.152.183 at 2:47:30PM EST. Open source search of IP Address 212.83.152.183 identified it as assigned to Tiscali Telecom French Registry, a French Telecommunications company.

31. On July 26, 2017 at 2:50PM EST, the actor emailed Belt “Margaret, For some reason the link doesn’t work, Can you resend tracking numbers. Brian”. After discussion possible responses with the FBI, Belt responded to the actor saying that the link was working for her but she was working from home that day. At 3:39PM EST, the actor responded saying

“Send the tracking details as numbers, this link doesn’t work. Also what time does it say it will be received by vendor”.

32. At 4:21:37 PM EST on July 26 2017, the cyber actor accessed the website from the IP Address 40.77.167.43, which (per open source search) is assigned to Microsoft Corporation. The actor accessed the website again at 4:21:30 PM EST and 4:21:52 PM EST from the IP Address 71.169.8.2. Open source search of the IP Address 71.169.8.2 identified it is assigned to MCI Communication Services, which is owned by Verizon Wireless.

33. On July 27, 2017 the actor accessed the website again from IP Address 107.181.69.223 at 4:46:48AM EST. Open source search of the IP Address 107.181.69.223 identified it is assigned to Contina Communications, a hosting provider headquartered in Nashville, Tennessee.

34. On July 27, 2017 at 11:20AM EST, the actor emailed Belt “Margaret, I need to know the status of the payment, It has not yet been received by vendor. Please Advise. Brian”.

35. On July 28, 2017, FBI Louisville, Lexington Resident Agency conducted an interview with J.C.Q. regarding the FedEx package she was supposed to receive. J.C.Q. provided that she had been in a relationship with a “Graham Donald”, whom she met on match.com, for over a year. According to J.C.Q., “Graham Donald” is a 58-year-old Army Ranger currently deployed to Afghanistan. In December 2016, “Donald” flew to Frankfort, KY to spend three days with J.C.Q. at her home, after which they flew to Australia together

for a week-long vacation. J.C.Q. provided that “Donald” does business with a number of companies and sends his earnings to a realtor in Australia in the pursuit of purchasing a rental property. “Donald” asked J.C.Q. to manage this aspect of his finances for him since he is deployed and cannot manage his funds remotely. The process has worked in the past as follows: “Donald” has his business profits sent to J.C.Q. via FedEx, she then drives the checks to the nearest branch of Regions Bank branch in Indiana with whom “Donald” has accounts with, and then J.C.Q. arranges for the money to be wired to an account in Australia while at Regions Bank. To date, J.C.Q. has done this process for three checks for the following amounts: \$24,000, \$23,000, and \$15,000.

36. For the purposes of this Search Warrant, the Affiant has only included emails relevant to establish probable cause for this affidavit.

37. This Search Warrant attempts to obtain legal authority to identify the user (hereinafter TARGET USER) of TARGET EMAIL. Given the near identical actions of the actor whom successfully executed a scheme to defraud on Gorbel using the email executive.office@management-securemailservers-office-portal.online and the actions of the actor using the target email to attempt to defraud Gorbel, your Affiant believes that TARGET USER is repeatedly stealing the identity of Gorbel, a victim company within the District of Western New York, for the means of committing mail and wire fraud.

38. As a sophisticated cybercriminal, the TARGET USER consistently takes steps to hide his/her true identity and the location from which he/she is connecting and communicating. The hyperlink sent to the cyber actor was accessed with six unique IP

Addresses within a 24-hour period. The IP Addresses resolve to multiple countries, domestic geographic areas, and Internet Service Providers, with one of the IPs resolving to a VPN service. Based on my training and experience investigating cyber crimes, this behavior is indicative of attempt to obfuscate the true IP Address of an individual.

39. The deployment of the NIT will occur through email communications with the TARGET USER, with consent from the victim company, Gorbel, and the Accounts Payable manager Belt. The FBI will provide an email attachment to the victim which will be used to pose as a screen shot of the FedEx tracking portal for the sent payment. The FBI anticipates the target user, and only the target user, will receive the email and attachment after logging in and checking emails. The subject will download the attachment which will deploy a technique designed to identify basic information of the TARGET USER's location. Your Affiant believes the TARGET USER will see the opportunity to obtain information on the location of their illegally acquired payment and download the attachment. The attachment will only be included to the email sent to the TARGET EMAIL and will not be sent to any other email address. Based on historical activity, the FBI anticipates TARGET USER will access the TARGET EMAIL only after accessing a proxy or VPN service. As such, the FBI's first attempt to identify basic information without a more advanced technique only identified IP addresses belonging to the proxy services and not to the target user's actual computer. For the email attachment approach, the FBI will use a document with an embedded image requiring the computer to navigate outside the proxy service in order to access the embedded item.

40. The general public will be protected from any violation of privacy through careful and direct deployment of the NIT to the specific target email. Following the sending of the NIT to the target user, the FBI will ensure the tool is removed from the victim employer's network. The FBI will maintain, at all times, ownership of the NIT.

THE REMOTE SEARCH TECHNIQUE

41. Based on my training, experience, and the investigation described above, I have concluded that using a NIT may help law enforcement locate the user of the target email. Accordingly, I request authority to use the NIT, which will be deployed via email to investigate any user who logs into the TARGET EMAIL on any computer.

42. If a computer successfully activates the request to download the embedded image, the FBI computer hosting that image will show that download. Given the TARGET USER's anonymity techniques via proxy service as well as general curiosity, the deployment of this technique may result in the TARGET USER downloading the image multiple times. In each case, the web server log of the FBI machine will only show the timestamp, originating IP Address, and User String.

43. The subject will open the attachment which will include an embedded image hosted on a server operated by the FBI. By opening the attachment, and exiting protected mode (requiring a second manual step), the user's computer will connect to the FBI server to access the image content and, in doing so, will pass IP address information to the destination web server. This operation will not include a search of the user's computer nor

will it include the downloading of code to the machine; rather, this operation will pass the IP address and user agent string much like an IP address and user agent string are passed when any user accesses any web site. Given that no content is being searched nor is any computer code executed locally on that machine, the Government does not believe that a Search Warrant is required to execute the Embedded Image Option. In an abundance of caution, coupled with the fact that the user will need to exit protected mode within the Microsoft Word application, the Government is requesting authorization through a Search Warrant.

44. Specifically, this technique is designed to collect the items described below and in Attachment B, i.e., 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, instrumentalities, contraband and fruits of violations of target offenses. This information may include the following:

- a. The computer's IP address (Internet Protocol Address). An IP Address is a unique numeric address used to direct information over the Internet. IPv4 addresses are written as a series of four groups of numbers, each in the range 0 – 255, separated by periods (e.g., 121.56.97.178). Conceptually, IP addresses are similar to telephone numbers in that they are used to identify computers that send and receive information over the Internet.
- b. The User Agent String. The User Agent String is a short string of information that web browsers and other applications send to identify themselves to the web servers. The User Agent String commonly identifies the browser version, software version, operating system version, and device type.
- c. No screenshots of any kind will be taken of the computer of the when the TARGET USER opens the attachment sent to the TARGET EMAIL.

45. Each category of information sought by the NIT may constitute and/or contain evidence of the crimes under investigation, including information that may help to identify the computer receiving the NIT and its user. The computer's true assigned IP address can be associated with an Internet service provider ("ISP") and a particular ISP customer. The user agent string can help identify a pattern of web browsing techniques used while conducting illegal activity.

46. Based on my training, experience, my consultation with forensic computer experts, and the investigation described herein, your Affiant knows that network level messages and information gathered directly from a sending computer can be effective in identifying a computer, its location and individual(s) using a computer. For instance, individual(s) using the Internet can use compromised computers or commercial services to conceal their true originating IP address and thereby intentionally inhibit their identification. For example, as mentioned earlier, the subject accessing the target email account used the services of a proxy or VPN service to mask the IP address from which they are logging on to the target emails accounts. Getting an IP address and other information directly from the computer being used by the subject can defeat such techniques but only if the user or computer logic is outside of a proxy network session when executing the NIT exploit. The NIT will cause the above-described information to be sent over the Internet to a computer controlled by the FBI who will analyze the resulting information.

TIME AND MANNER OF EXECUTION OF THE SEARCH

47. Rule 41(e)(2) of the Federal Rules of Criminal Procedure requires that the 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” The government seeks permission to deploy the NIT at any time of day or night within 14 days of the date the warrant is authorized. There is good *cause* to allow such a method of execution as the time of deployment causes no additional intrusiveness or inconvenience to anyone. More specifically, the government has no control of the timing or when the subject(s) will access the target emails accounts. The government also seeks to read any the information that the NIT causes to be sent from the activating computer at any time of day or night during the 14 days from the date the warrant is authorized. This is because the individuals using the activating computer may activate the NIT after 10:00 PM or before 6:00 AM and law enforcement would seek to read the information it receives as soon as it is aware of the NIT response.

JURISDICTION

48. This Court has jurisdiction to issue the requested warrant under Rule 41(b)(6)(A) because the above facts establish there is probable cause to believe that the location of the computer accessing the target emails has been concealed through technological means, and that there is probable cause to believe that activities related to the crime being investigated occurred within this judicial district.

AUTHORIZATION REQUEST; DELAYED NOTICE

49. Pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), I request that this Court authorize the officers executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed.

50. This application seeks a warrant authorizing the use of computer software on the computer accessing the target email that, after successful installation, will collect and send information from that computer and make it available to government personnel authorized by the requested warrant to receive and review such information. Thus, the warrant applied for would authorize the copying of electronically stored information under Rule 41(e)(2)(B). However, as further specified in Attachment B, which is incorporated into the warrant, the applied-for warrant does not authorize the physical seizure of any tangible property.

51. It is intended that the collection and sending of such information will be performed without the knowledge of the target user.

52. 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. Providing immediate notice to the owner or user of the target emails would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. See 18 U.S.C. § 3103a(b)(1).

53. To the extent that Attachment B describes stored wire or electronic information, such a seizure is reasonably necessary, because without this seizure, there would be no other way, to my knowledge, to view the information and to use it to further the investigation. Furthermore, the network investigative technique does not deny the users or administrators access to the account information, nor does the technique permanently alter any of the information stored in the accounts. See 18 U.S.C. § 3103a(b)(2).

SEARCH AUTHORIZATION REQUESTS

54. Accordingly, for each of the aforementioned reasons, it is respectfully requested that this Court issue a search warrant authorizing the following:

- a. the NIT may cause an activating computer – wherever located – to send to the FBI network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer;
- b. that the government may receive and read, at any time of day or night, within 14 days from the date the Court authorizes the use of the NIT, the information that the NIT causes to be sent to the computer controlled by the FBI;
- c. that, pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(f)(3) of the Federal Rules of Criminal Procedure, the government may delay providing a copy of the search warrant and the receipt for any property taken until the time that a suspect has been identified and has been placed in custody from the sending of the NIT unless notification is further delayed by the court; and
- d. that provision of a copy of the search warrant and receipt may, in addition to any other methods allowed by law, be effectuated by electronic delivery of true and accurate electronic copies (e.g., Adobe PDF file) of the fully executed documents in the same manner as the NIT is delivered.

REQUEST FOR SEALING

55. It is respectfully 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 this document is necessary because the search warrant is relevant to an ongoing investigation. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

CONCLUSION

56. Based on the information identified above, information provided to me, and my experience and training, I have probable cause to believe there exists evidence, instrumentalities, contraband and fruits of criminal activity related to the stalking and targeted unauthorized computer access on computers that access target emails, in violation of Title 18, United States Code, Sections 1028A (Aggravated Identity Theft), 1341 (Frauds and Swindles), 1343 (Wire Fraud), and 1349 (Attempts and Conspiracy).

57. Based on the information described above, there is probable cause to believe that the information described in Attachment B constitutes evidence of these crimes.

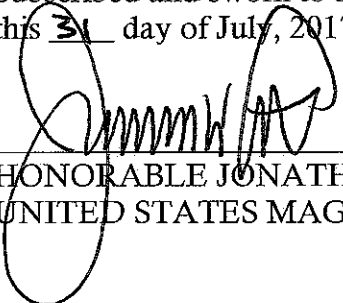
58. Based on the information described above, there is probable cause to believe that deploying the NIT on the computer described in Attachment A, to collect information described in Attachment B, will result in the United States obtaining the evidence and instrumentalities of the target offenses described above.

Respectfully submitted,



Meredith McClatchy, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 31 day of July, 2017



HONORABLE JONATHAN W. FELDMAN
UNITED STATES MAGISTRATE JUDGE