UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with mistergrey@live.ru that is stored at premises controlled by Microsoft

Case No. 14-M-509

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:

See Attachment A.

over which the Court has jurisdiction pursuant to Title 18, United States Code, Sections 2703 and 2711, there is now concealed:

See Attachment B.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ■ 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 violations of: 18 U.S.C. § 1030 and 1037.

The application is based on these facts: See attached affidavit.

☐ 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 affidavit.

Applicant's signature

Eliot Mustell, Special Agent, Federal Bureau of Investigation
Printed Name and Title

Sworn to before me and signed in my presence:

Date: December 30, 2014 at 2:45 PM

Judge's signature

City and State: Milwaukee, Wisconsin

William, E Callahan, Jr., U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF
APPLICATIONS FOR SEARCH WARRANTS

I, Eliot J. Mustell, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Microsoft Corporation, ("Microsoft"), an email provider headquartered in Redmond, Washington and at AOL, an email provider headquartered in Dulles, Virginia. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of applications for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft and AOL to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation. I have been employed with the FBI since February 2013. I am currently assigned to the FBI Milwaukee Division's Cyber Crimes Task Force. Prior to becoming a Special Agent with the FBI, I have worked in a variety of private positions in the Information Technology industry. As a Special Agent with the FBI, I investigate criminal and national security related computer intrusion matters involving botnets, distributed denial of service attacks, the distribution of SPAM, malicious software, the theft of personally identifiable information, and other computer related fraud. Since joining the FBI, I have been involved in numerous criminal and national security investigations involving computer intrusions. I have received education and training in computer technology, and computer-based fraud; and I have held industry certifications from Cisco, EC

Council, and Microsoft.

3. 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.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1030(a)(5)(fraud and related activity in connection with computers) and 1037 (violations of the CAN-SPAM Act) have been committed by unknown persons. There is also probable cause to search the information described in Attachment A for evidence and instrumentalities of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. As part of ongoing investigations into cyber criminal activities, U.S. authorities contacted Alexander Holden, Chief Information Officer of Hold Security LLC, Milwaukee, WI after an interview of Holden appeared in the New York Times newspaper on August 5, 2014. According to the interview, Holden had obtained information that a "Russian crime ring" had amassed the largest yet seen collection of stolen Internet credentials, to include 1.2 billion username and password combinations, and more than 500 million e-mail addresses. According to Holden, the collection was discovered by Hold Security, a cyber-security firm located in Milwaukee, Wisconsin and operated by Alexander Holden. Based on follow-up information

provided to U.S. authorities, Holden stated that "Cyber Vor," a Russian-based hacker group, was responsible for obtaining these credentials or for compromising the computer systems that resulted in obtaining these credentials.

7. Holden stated that he obtained this information from self-proclaimed hackers or from finding databases on various online hacking forums which contained compromised account information. Additionally, Holden stated that his competition works by establishing and monitoring "listeners" set up on other hacker's networks. However, Holden stated that he would not discuss the specifics of his methodologies as it would violate service level agreements or jeopardize his business.

8. On August 15, 2014, Holden provided the FBI with 263GB of raw text files containing all of the stolen credentials. A review of this information revealed text files containing, inter alia: username and pass phrase credentials, credit card information, Social Security numbers, e-mail addresses, and File Transfer Protocol ("FTP") accounts.

9. Analysis of the data provided by Holden also revealed lists of domain names (a unique name which identifies an internet resource such as a website) in the data. Based on a review of these domain names and their locations within the files, I believe that the domain names are likely being used to send spam emails. Case agents also located several executable files (i.e., programs) within the data. These executables appear to be utilities for sending spam email and using Structured Query Language ("SQL") injection to exploit security vulnerabilities within victim application's software.

10. During analysis of the data, the email addresses mistergrey@live.ru and sdcltd@aol.com were located within areas of the data that reflected computer intrusion (hacking) activity. Specifically, they were located in spamming utilities as being test email addresses. Test

email addresses allow a spammer to send email to the test accounts to verify that the spam is working correctly. Spammers will then access the test email accounts to ensure that the spam is formatted correctly, before distributing spam to real victims. Using these utilities and test email accounts allows the spammer to control the quality of spam messages and troubleshoot any potential issues with the spamming utilities.

11. Based on my training and experience, I am aware that in some spamming utilities, the test email entry field is left blank to allow the user to input their own email address. However, in the data provided by Holden, the email addresses, mistergrey@live.ru and sdcltd@aol.com, were pre-populated in the test email field. Because the test email field was pre-populated, I believe that the author of this utility either modified the source code or the associated configuration file of the utilities in advance, to preventing the user from needing to manually input test email accounts prior to execution. Additionally, both utilities located in the data provided by Holden functioned similarly, in that they each had a field to browse to a list of victim accounts to spam, and a proxy field to aid in obfuscating the users originating IP address when using this utility. As a result, I believe that accessing the contents of these two email addresses will assist in determining the identity of the hacking ring, as it will allow law enforcement to see what types of spam emails were being sent and trace the emails back to a particular type of malware, spamming utility or affiliate network.

12. On or about October 2, 2014, Microsoft provided subscriber information for the email account mistergrey@live.ru, in response to a subpoena. According to records obtained from Microsoft, email address mistergrey@live.ru was registered on May 24, 2010, from IP address 83.133.122.142. According to a Whois query, this IP address resolved to a virtual private server (VPS) and domain hosting company. Based on my training and experience, I am

aware that hackers will frequently use a VPS in an attempt to obfuscate their originating IP address without compromising network throughput. The hacker will then launch attacks and related activities from a VPS leased often under an alias, which makes it more difficult for law enforcement to track their true location as law enforcement must then obtain the connection logs to the VPS in order to find the originating IP address of the hacker. Erasing or wiping a VPS is also much easier than wiping a physical computer and can be done remotely with little effort.

13. Additionally, the subpoena response from Microsoft indicated that the user who created the email account listed the user's State as Kursk, and the user's country as Russia. Kursk is a town in the south western part of Russia.

14. According to records obtained from Microsoft, between January 3, 2014, and July 14, 2014, there were 25 logins to the e-mail address mistergrey@live.ru. Each of the logins was from IP address 212.117.172.100. A search of CentralOps.net for IP address 212.117.172.100 revealed that the IP address 212.117.172.100 resolves to Root S.A., a leading internet backbone and co-location provider specialized in dedicated servers, co-location, and web hosting located in Luxembourg. Based on my training and experience, I am aware that individuals involved in spamming activities will either legally obtain server space, or illegally hack into servers to use as part of the command and control function or their botnets or to hide their locations and identities.

15. In general, I am aware that an email that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Microsoft servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Microsoft's servers for a certain period of time. In addition, a preservation letter was sent to Microsoft, Inc., for the contents of the email account mistergrey@live.ru on October 2, 2014.

16. Based on my training and experience, I am aware that hackers and spammers will frequently re-use online nicknames or monikers in order to create a consistent online identity. As part of this investigation, case agents logged into a known online Russian hacking forum "exploit.in" to determine whether either of these email addresses were related to online monikers who used these forums for spam-related activities. On this forum, a user who used the online moniker "mr.grey" was located.

17. During the review of the hacking forum "exploit.in," case agents observed a number of posts by and to "mr. grey." In a post dated April 11, 2011, a user asked how much it would cost to obtain hacked accounts for social network sites, including Facebook, Twitter and VK (VK stands for VKontakte, is a Russian social networking site similar to Facebook). On November 30, 2011, "mr.grey" responded that if anyone is still interested in obtaining access to hacked accounts on these sites, he/she could gather up some. On or about November 30, 2011, a user asked how to handle a victim's complaint about spamming and malware. The user "mr.grey" responded by saying there is no template on how to handle victim complaints.

18. Case agents also researched the second test email address found in the spamming utility of the data provided by Alex Holden. The email address sdcltd@aol.com was located as the contact email address for the Facebook profile under the name of Fereydon Abdollahyan, located in Great Britain. According to records obtained from AOL, the subscriber information for the e-mail address sdcltd@aol.com is a Fereydon Abdollahyan, located in West Wickham Kent, BR4 9JZ in Great Brittan. Additionally, on November 17, 2014, case agents attempted to create a new AOL email account sdcltd@aol.com, but received a message from AOL stating "Sorry, this username is taken." This message is indicative of the email account sdcltd@aol.com already existing at AOL.

19. In general, I am aware that an email that is sent to an AOL subscriber is stored in the subscriber's "mail box" on AOL servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on AOL servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on AOL's servers for a certain period of time. Additionally, a preservation letter was sent to AOL, Inc., for the above mentioned account on November 17, 2014.

BACKGROUND CONCERNING EMAIL

20. In my training and experience, I have learned that Microsoft provides a variety of on-line services, including electronic mail ("email") access, to the public. Microsoft allows subscribers to obtain email accounts at the domain name live.ru, including the email account listed in Attachment A. Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic communications (including retrieved and non-retrieved email for Microsoft subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

21. A Microsoft or AOL subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, screen names, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Microsoft. In my training and experience, evidence of who was using an email account may be

found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

22. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

23. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

24. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

25. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either

inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

26. Based on the forgoing, I request that the Court issue the proposed search warrants. Because the warrants will be served on Microsoft and AOL who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A - Microsoft

Property to Be Searched

This warrant applies to information associated with mistergrey@live.ru that is stored at premises controlled by Microsoft, a company that accepts service of legal process at Microsoft Corp, One Microsoft Way, Redmond, WA 98052.

ATTACHMENT B - Microsoft

Particular Things to be Seized

I. Information to be disclosed by Microsoft (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on October 2, 2014, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, screen names, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1030(a)(5)(fraud and related activity in connection with computers) and 1037 (violations of the CAN-SPAM Act), those violations involving unknown individuals and occurring in or after 2011, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Communications related to sending spam email messages.

b. Communications related to malware and/or computer viruses.

c. Communications related to computer botnets.

d. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

e. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

f. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

g. The identity of the person(s) who communicated with the email address mistergrey@live.ru about matters relating to computer intrusions or spamming, including records that help reveal their whereabouts.

ATTACHMENT A – AOL

Property to Be Searched

This warrant applies to information associated with sdcltd@aol.com that is stored at premises controlled by AOL, a company that accepts service of legal process at AOL, Inc., 22000 AOL Way, Dulles, VA 20166.

ATTACHMENT B – AOL

Particular Things to be Seized

II. Information to be disclosed by AOL (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 17, 2014, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, screen names, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1030(a)(5)(fraud and related activity in connection with computers) and 1037 (violations of the CAN-SPAM Act), those violations involving unknown individuals and occurring in or after 2011, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Communications related to sending spam email messages.

b. Communications related to malware and/or computer viruses.

c. Communications related to computer botnets.

d. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

e. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

f. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

g. The identity of the person(s) who communicated with the email address sdcltd@aol.com about matters relating to computer intrusions or spamming, including records that help reveal their whereabouts.