

DSS: CMP
F.#2012R00556

13 M 0 13

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - -X

UNITED STATES OF AMERICA

AFFIDAVIT AND COMPLAINT IN
SUPPORT OF ARREST WARRANT
AND SEARCH WARRANT

- against -

MICHAEL MENESES,

(T. 18, U.S.C., §§ 1030;
Fed. R. Crim. P. 41)

Defendant.

- - - - -X

IN THE MATTER OF AN APPLICATION
FOR A SEARCH WARRANT FOR THE
PREMISES KNOWN AND DESCRIBED AS 81
MAPLE AVENUE, APARTMENT 1,
SMITHTOWN, NEW YORK 11787

- - - - -X

EASTERN DISTRICT OF NEW YORK, SS:

RAYMOND MILLER, being duly sworn, deposes and states
that he is a Special Agent of the Federal Bureau of Investigation
("FBI"), duly appointed by law and acting as such.

UNLAWFUL TRANSMISSION OF COMPUTER CODE AND COMMANDS

In or about and between December 2011 and May 2012,
both dates being approximate and inclusive, within the Eastern
District of New York and elsewhere, the defendant MICHAEL MENESES
did knowingly and intentionally cause and attempt to cause the
transmission of information and one or more programs, codes and
commands, to wit: system commands, and as a result of such
conduct, did intentionally cause damage without authorization to

one or more protected computers, to wit: computers belonging to a company that manufactures high-voltage electronics, which offense caused, and if completed would have caused, loss to one or more persons during a one-year period aggregating at least \$5,000 in value, and damage affecting ten or more protected computers during a one-year period.

(Title 18, United States Code, Section 1030(a)(5)(A))

APPLICATION FOR SEARCH WARRANT

Upon information and belief, there is probable cause to believe that there is located in THE PREMISES KNOWN AND DESCRIBED AS 81 MAPLE AVENUE, APARTMENT 1, SMITHTOWN, NEW YORK 11787 (the "PREMISES"), further described in Attachment A, the things described in Attachment B, which constitute evidence, fruits and instrumentalities of the unlawful transmission of information and one or more programs, codes and commands to protected computers and of the unauthorized access of protected computers, in violation of Title 18, United States Code, Section 1030.

The source of your deponent's information and the grounds for his belief are as follows:

1. I have been a Special Agent with the FBI since 2007. I am assigned to an FBI squad tasked with investigating cybercrime, including network intrusions and other forms of unauthorized access to computer networks, identity theft, wire

fraud, bank fraud, access device fraud and other computer-based crimes.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from, among other things: (a) my personal participation in this investigation, (b) reports made to me by other law enforcement agents and agencies, (c) interviews of victims and witnesses, (d) my review of network audit logs and other forensic evidence, and (e) my review of other records obtained pursuant to grand jury subpoenas and of publicly-available information. Except as explicitly set forth below, I have not distinguished in this affidavit between facts of which I have personal knowledge and facts of which I have hearsay knowledge. Because this affidavit is being submitted for the limited purpose of establishing probable cause for the arrest of the defendant MICHAEL MENESES and search of the PREMISES, I have not set forth each and every fact learned during the course of this investigation. Instead, I have set forth only those facts that I believe are necessary to establish probable cause for the arrest and search warrant.

PROBABLE CAUSE TO ARREST

A. Background

3. From approximately May 2008 through January 2012, MENESES was employed as a software programmer and system manager for a company based in Suffolk County, New York, that manufactures high voltage power supply materials and other products (the "Victim Company"). Among other positions, MENESES held the title of Glovia System Manager at the Victim Company. Glovia is a software solution for enterprise resource planning ("ERP"), and is used in connection with purchasing, inventory control, production, production planning, accounting and sales, among other things. Glovia source code can be customized to meet the needs of a particular system, and during his employment at the Victim Company, MENESES and one of his colleagues, "John Doe," were responsible for, among other things, writing programming code, procedures and scripts to enhance various processes for the Victim Company's ERP system. In the 2011-2012 time period, MENESES and John Doe were the primary employees of the Victim Company responsible for the development and customization of Glovia source code. Among other things, MENESES and John Doe worked on developing scripts that would enable the Glovia system to be updated automatically to correspond to a bar code scanning function. In this script development process, John Doe shared one of his passwords with MENESES on at least one

occasion. Specifically, on or about August 9, 2011, John Doe emailed a Windows batch file¹ to MENESES that would be used to call a Glovia task to perform a purchase order receipt transaction. In this batch file, John Doe embedded his user name and password into the text. In the 2011-2012 time period, John Doe would use the same passwords for the Glovia system and other systems that required log-in credentials. Such passwords would be changed approximately every 90 days, and it was John Doe's practice to rotate among the same two or three passwords each time he was required to change his password.

4. During his employment with the Victim Company, MENESES was able to access the Victim Company's servers remotely through the Victim Company's virtual private network ("VPN"), which allowed him to log on from home and elsewhere.

5. On or about December 30, 2011, MENESES tendered his resignation to the Victim Company and identified his last working day as January 13, 2012. MENESES had previously expressed his displeasure at being passed over for promotions, among other issues.

6. On or around Friday, January 6, 2012, MENESES's supervisor (the "Supervisor") observed MENESES copying files from his computer onto a flash drive. The Victim Company's network

¹ A batch file is a text file containing a series of commands to be executed by the user.

operations unit created a report of the copied files, which included, inter alia, various programs and procedures that MENESES and others had created for the Victim Company's Glovia system, as well as other processes and systems, such as custom cost processing, purchase order systems, inventory systems and work order processing for the Victim Company's overseas suppliers. In addition to these items, MENESES was also found to have transferred employment documents involving a large multinational company with a location in Cary, North Carolina (the "New Employer"), which indicated he was taking a position with the New Employer.

7. As a result of MENESES's actions, on or about January 7, 2012, the Victim Company blocked his access to the company's data center and denied him access to the VPN and another remote access system. During the same time period, MENESES was also removed from the network's administrative group, and the Victim Company created explicit denials for every access server to the Victim Company's system, such that MENESES could not use his own log-in credentials to access the Victim Company's network. MENESES's authorized access to all Victim Company information was terminated at approximately 2:00 p.m. EST on January 13, 2012, his last day of employment at the Victim Company.

B. Unauthorized Access to John Doe's Email Account

8. On or about January 31, 2012 at approximately 2:57 p.m. EST, a candidate for the position that MENESES had vacated at the Victim Company (the "Candidate") sent an email to the Supervisor's work email account regarding the new position. The Supervisor forwarded the Candidate's email to John Doe's work email account at approximately 3:04 p.m. EST. Approximately 15 minutes later, at 3:19 p.m. EST, the Candidate received an email from "iamconcern2012@gmail.com" that simply stated, "Dont [sic] accept any position from [the Victim Company]." This Gmail account was created on January 31, 2012 at 3:17 p.m. EST, and the subscriber name is "glovia glovia." The Internet Protocol ("IP") address used to create this Gmail account at that date and time resolved to a subsidiary of the New Employer.

9. Based on my experience investigating network intrusions and unauthorized email access, I believe that MENESES obtained unauthorized access to John Doe's email account, read the email regarding the Candidate, and quickly created the "iamconcern2012@gmail.com" account to discourage the Candidate from applying. MENESES likely obtained this unauthorized access to John Doe's email account through one of several methods. For example, MENESES may have used the password for John Doe that was transmitted to him in the August 9, 2011 batch file described above in paragraph 3, given that John Doe regularly re-used

passwords. In addition, later investigation revealed that on or about December 14, 2012, an unauthorized Database System Identification ("DBSYSID") lookup program was created by a user under the name "MM4." This DBSYSID lookup program was created to look up and return Glovia and Oracle (a database program) connection information, including the associated passwords, to "MM4." Thus, I believe that MENESES may have had an opportunity to learn John Doe's email password by creating the DBSYSID lookup program (the "MM" in user name "MM4" likely refers to "Michael Meneses") and then using that program to record John Doe's password when John Doe accessed the Oracle or Glovia systems.

C. Transmission of Unauthorized Commands to the Victim Company's System

10. On or about February 1, 2012 (the day after the Victim Company's month-end closing), the ERP department received a number of calls from users around the company indicating that they were unable to process routine transactions and were receiving error messages. After investigating this problem, the Victim Company determined that the secure periods for production and finance were rolled into March instead of February - in other words, the beginning of the new month had been postponed to March 1, 2012 (instead of February 1, 2012). The Victim Company's network audit logs indicate that at approximately 10:57 p.m. on

January 31, 2012, an individual used John Doe's credentials to change the "BEG_DATE" (beginning date) of the Period Roll table to March 1, 2012 from February 1, 2012, and changed the "END_DATE" (end date) to March 31, 2012 from February 29, 2012. John Doe, however, had already made the appropriate changes to the Period Roll table (changing the beginning date to February 1, 2012 from January 1, 2012, and the end date to February 29, 2012 from January 31, 2012) at approximately 8:38 p.m. and left the premises of the Victim Company at approximately 10 p.m. or shortly before 10 p.m.

11. The modifications to the Period Roll table made at 10:57 p.m. originated from an IP address that resolved to the Residence Inn Hotel in Cary, North Carolina (the "Residence Inn"), which is a short distance from the New Employer's location in Cary, North Carolina. The Residence Inn's records indicate that MENESES was staying at that hotel from January 29, 2012 to February 4, 2012. Based on this information and the information described above about MENESES's access to John Doe's credentials, as well as my experience investigating network intrusions and other forms of unauthorized access to computer networks, I believe that MENESES used John Doe's credentials to remotely access the Victim Company's system from the Residence Inn and to send the commands modifying the Period Roll table that damaged the system.

12. The Victim Company also determined that the log-in credentials of John Doe and an outside Glovia consultant who had not accessed his user account at the Victim Company for approximately one year were used to log into the Victim Company's network via VPN multiple times from January 21, 2012 to January 27, 2012. Each of these log-ins occurred from an IP address that resolves to an Optimum Online account subscribed to "Mike Meneses" with the same address as the PREMISES. Thus, there is probable cause to believe that MENESES was accessing the Victim Company's system remotely via his residential Optimum Online account without authorization.

13. The Victim Company has identified several other incidents of unauthorized access and unauthorized commands sent to its system in the same time period as MENESES's unauthorized access into the Victim Company's system, which occurred from approximately January 10, 2012 through February 3, 2012 (the "Breach Period").^{2/} These incidents appear to be associated with MENESES given their timing and the types of systems that were affected. Among other things, various audit triggers were deleted during the Breach Period, and a purchase order table was

² Although the breach was resolved on or about February 1, 2012, additional attempts were made to gain unauthorized access to the Victim Company's system using the credentials of John Doe and the Glovia consultant described above through February 3, 2012.

manually purged on or about Tuesday, January 31, 2012 (the purging process was typically done automatically on Fridays), which prevented the Victim Company from converting purchase requisitions to purchase orders on February 1, 2012. In May 2012, the Victim Company discovered that a line of code in a software program that calculates work order costs was deleted on or about January 18, 2012, which led to the incorrect calculation of these costs.

14. The Victim Company estimates that it has incurred approximately \$94,000 in investigative, forensic and remedial costs, among other damages suffered by the company, as a result of MENESES's breach of the Victim Company's network.

APPLICATION FOR SEARCH WARRANT

A. The PREMISES

15. The residence located at the PREMISES is a red-brick, two-story duplex building with two adjacent but separate entry doors in the front of the building. A photograph generated by Google is attached hereto as Exhibit 1. I conducted surveillance at the PREMISES on or about March 21, 2013 and observed MENESES standing in the doorway of the PREMISES. Additionally, MENESES's Optimum Online subscriber information list his address as of April 25, 2012 as "81 MAPLE AV APT 1, Smithtown, NY 11787," and records received from National Grid on behalf of the Long Island Power Authority indicate that the

electric customer account for 81 Maple Avenue, Smithtown, New York 11787 is listed in the name "Michael Meneses."

16. As described in the preceding section, there is probable cause to believe that the PREMISES contain, at a minimum, at least one personal computer and/or other electronic device and modem, which were used to facilitate MENESES's remote unauthorized access into the Victim Company's system and transmission of unauthorized commands thereto, and attempts to do so, on multiple occasions during the Breach Period. Moreover, in light of MENESES's computer expertise, there is also probable cause to believe that the PREMISES will contain other storage media (such as the flash drive onto which MENESES transferred the Victim Company's data, as described above), a wireless router and other electronic devices that may have been used to facilitate his criminal activity during the Breach Period or that may contain communications indicating his motive for committing the criminal activity described herein, such as his dissatisfaction with his employment at the Victim Company.

B. Records Sought

17. As described above and in Attachment B, this application seeks permission to search for all records that might be found on the PREMISES, in whatever form they are found, that contain evidence of MENESES's criminal activity. One form in which the records might be found is data stored on a computer's

hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Fed. R. Crim. P. 41(e)(2)(B).

18. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the storage medium that is not currently being used by an active file - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media - in particular, computers' internal hard drives - contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating

system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

19. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that attribute this evidence to MENESES - in other words, to demonstrate how the computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in

which they were created, although this information can later be falsified.

- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.
- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how the computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs

(and associated data) may be relevant to establishing the user's intent.

- f. I know that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

20. In most cases, a thorough search of a premises for information that might be stored on storage media often requires agents to seize physical storage media and later review the media consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of

documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on the Premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

21. Based on the foregoing, and consistent with Fed. R. Crim. P. 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of

the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

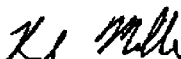
22. In conclusion, based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the PREMISES there exists evidence of crimes.

WHEREFORE, your deponent respectfully requests that an arrest warrant be issued for the defendant MICHAEL MENESES so that he may be dealt with according to law.

WHEREFORE, your deponent further respectfully requests that the requested search warrant be issued for THE PREMISES KNOWN AND DESCRIBED AS 81 MAPLE AVENUE, APARTMENT 1, SMITHTOWN, NEW YORK 11787.

FURTHER, your affiant requests that the Court order that this Complaint and Affidavit in Support of Application for Arrest Warrant and Search Warrant, as well as any arrest warrant and search warrant issued pursuant to this document, be sealed, until further order of the Court, to avoid alerting the defendant to the existence of this investigation and arrest and search warrant, which could result in his flight from prosecution and the destruction of the evidence sought herein.

Dated: Brooklyn, New York
April 18, 2013



RAYMOND MILLER
Special Agent
Federal Bureau of Investigation

Sworn to before me this
18th day of April, 2013

THE HONORABLE JOAN M. AZRACK
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

EXHIBIT 1
81 Maple Avenue
Smithtown, New York 11787
(the PREMISES)

Google

Address **Maple Avenue**

Address is approximate



ATTACHMENT A

Property to Be Searched

The property to be searched is THE PREMISES KNOWN AND DESCRIBED AS 81 MAPLE AVENUE, APARTMENT 1, SMITHTOWN, NEW YORK 11787, further described as a two-story red brick residential building with two entry doors in the front of the building.

ATTACHMENT B
Property to be Seized

1. All records^{1/} relating to violations of 18 U.S.C. § 1030 involving MICHAEL MENESES, including computers^{2/} and storage media^{3/} that contain or in which are stored records or information (hereinafter "COMPUTERS") used as a means to commit violations of 18 U.S.C. § 1030. All information obtained from such computers or storage media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 1030 involving MICHAEL MENESES, including:

a. evidence of who used, owned, or controlled the COMPUTERS at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, correspondence and network configuration, including any virtual private network (VPN), Citrix or other remote access configurations;

¹ As used herein, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form.

² As used herein, the term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

³ As used herein, the term "storage medium" includes any physical object upon which computer data can be recorded. Examples include external hard drives, flash drive and other forms of flash memory, hard disks, RAM, CDs, DVDs and other magnetic optical media.

- b. evidence of software that would allow others to control the COMPUTERS, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the COMPUTERS of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTERS was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTERS;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTERS;
- i. contextual information necessary to understand the evidence described in this attachment;

2. Records and things evidencing the use of the Internet Protocol ("IP") address 24.184.7.222 and/or any other IP addresses associated with 81 MAPLE AVENUE, APARTMENT 1, SMITHTOWN, NEW YORK 11787 in connection with and/or in furtherance of violations of 18 U.S.C. § 1030 involving MICHAEL MENESES, including:

- a. routers, modems, and network equipment used to connect computers to the Internet;
- b. IP addresses used by the COMPUTER;
- c. records or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

all of which constitute evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030.