SEALED

UNITED STATES DISTRICT COURT

for the

Western District of Virginia

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

Zachary Shames at James Madison Univ., Shenandoah Hall, Rm B305, 1671 Carrier Drive, Harrisonburg, VA

Case No. 5:15mj00018

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 person known as Zachary Shames more particularly described in Attachment A of the attached Affidavit and hereby incorporated by reference as if fully stated herein

located in the Western District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B of the attached Affidavit, incorporated herein by reference.

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

☑ evidence of a crime;

☑ contraband, fruits of crime, or other items illegally possessed;

☑ property designed for use, intended for use, or used in committing a crime;

□ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC § 1030	Computer fraud
18 USC § 1343	Wire fraud
18 USC §§ 371, 2	Conspiracy and aiding and abetting

The application is based on these facts:
See Attachment B of the attached affidavit, incorporated herin by reference.

☑ 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

Special Agent Peter M.D. Vu
Printed name and title

Sworn to before me and signed in my presence.

Date: 03/16/2015

Judge's signature

City and state: Harrisonburg, VA

Hon. Joel Hoppe, United States Magistrate Judge
Printed name and title

SEALED

IN THE
UNITED STATES DISTRICT COURT
FOR THE
WESTERN DISTRICT OF VIRGINIA
HARRISONBURG DIVISION

IN THE MATTER OF THE SEARCH OF THE PREMISES LOCATED AT JAMES MADISON UNIVERSITY, SHENANDOAH HALL ROOM B305, 1671 CARRIER DRIVE, HARRISONBURG, VIRGINIA 22807, AND THE PERSON OF ZACHARY LEE SHAMES	Case No. 5:15mj00018 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Peter M.D. Vu, being duly sworn, state:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") assigned to the Washington Field Office, where my current duties include the investigation of computer crimes. I have been employed as a Special Agent with the FBI for over 18 years. As a Special Agent, I have received training in, and have investigated, crimes involving computers, fraud, and intellectual property rights. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, intellectual property and other computer based crimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have participated in the execution of many search warrants.

2. I make this affidavit in support of an application for a search warrant to search the James Madison University (JMU) dorm room of ZACHARY LEE SHAMES located at Shenandoah Hall Room B305, 1671 Carrier Drive, Harrisonburg, Virginia 22807 (hereinafter the "SUBJECT PREMISES") and person of ZACHARY LEE SHAMES, as further described in Attachment A, because there is probable cause to believe that the SUBJECT PREMISES contain

evidence, fruits, and instrumentalities of violations, or attempted violations, of Title 18, United States Code, Sections 1030 (computer fraud), 1343 (wire fraud), 371 (conspiracy), and 2 (aiding and abetting).

3. The facts in this affidavit are from my personal observations, my training and experience, and information obtained from other agents and witnesses. 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, I submit that there is probable cause to believe that violations of Title 18, United States Code, Sections 1030 (computer fraud), 1343 (wire fraud), 371 (conspiracy), and 2 (aiding and abetting) have been committed by various individuals, including an individual at the SUBJECT PREMISES. I submit that there is also probable cause to believe that the SUBJECT PREMISES contain or on the person of ZACHARY LEE SHAMES there are items described in Attachment B hereto, all of which constitute evidence, fruits, and instrumentalities of violations of these crimes, as further described in Attachment B.

RELEVANT STATUTES

5. *Fraud in relation to computers*. Title 18, United States Code, Section 1030 provides, in relevant part, that whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer; or whoever knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value exceeding $5,000 during any 1-year period; or whoever intentionally accesses a protected computer without authorization, and as a result of such

conduct, causes damage and loss, shall be guilty of a federal offense. 18 U.S.C. §§ 1030(a)(2), (4), (5).

6. *Wire Fraud.* Title 18, United States Code, Section 1343 provides that whoever, "having devised 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 a wire... in interstate of foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice" is guilty of a federal offense.

7. *Conspiracy.* Title 18, United States Code, Section 371 provides that "[i]f two or more persons conspire either to commit any offense against the United States... and one or more of such persons do any act to effect the object of the conspiracy, each" is guilty of a federal offense.

8. *Aiding and abetting.* Title 2, United States Code, Section 2 provides that "[w]hoever commits an offense against the United States or aids, abets, counsels, commands, or induces or procures its commission, is punishable as a principal."

SUMMARY OF PROBABLE CAUSE

9. This investigation relates to individuals who are involved in the development and distribution of the Limitless Keylogger and Syndicate Stealer malware (malicious spyware). One of the individuals, who appears to be a developer of the Limitless Logger, has been identified as , ZACHARY LEE SHAMES, a student at JMU which is located in Harrisonburg, Virginia, in the Western District of Virginia.

10. During this investigation, I have obtained information that users of the Limitless Keylogger have targeted small to medium size companies located in many countries around the

world. The users appear to be targeting companies with publicly-available contact information likely obtained from corporate websites. After the users choose their targets, the users send them business-themed emails with social engineering lures to trick unwitting email recipients at the companies into unknowingly downloading and executing the attachment to install the keylogger. Once the keylogger has been executed, the keylogger steals victim computer system information, keystrokes, browser-cached account credentials for websites. As such, the keylogger users are able to invade their victims' privacy and, in the case of corporate victims, monitor the victim company or business activities in furtherance of fraud.

11. Specifically, targeted individuals and entities have included those in the manufacturing sector, health industry, governmental agencies, non-governmental organizations, and financial institutions, including those located in Canada, Jordan, Cambodia and the United Arab Emirates. Many of the targeted phishing emails (emails designed to trick unsuspecting users into disclosing personal identifying information or passwords) were sent to company email accounts, such as info@<company domain name>, admin@<company domain name>, and sales@<company domain name>. If the unwitting recipient opens the email attachment resulting in the execution of the keylogger, the malware then begins collecting victim information, including usernames and passwords, without the victim's authorization or knowledge. Armed with the stolen information, the individual or individuals deploying the keylogger can engage in subsequent attacks, including theft of online banking information and hijacking victim email accounts.

12. This investigation has confirmed that the Limitless Keylogger was offered on the website http://limitlessproducts.org. The keylogger can be purchased from this website and from an underground forum using PayPal as the method of payment. A subject of a FBI investigation

purchased the keylogger for $25 via PayPal. FBI agents also obtained information that the keylogger was being sold in the underground market for $40 or less. Additionally, both the Limitless Keylogger and Syndicate Stealer malware products were offered on the website http://nitroproducts.info. The contact email address listed on the nitroproducts.info website to obtain product support was jkbest22@gmail.com. Based on my training and experience, this email address would have received support-type questions or questions pertaining to the product, and likely would have sent responses to those questions.

13. The Limitless Keylogger and Syndicate Stealer are both malware programs which monitor keystrokes from the infected computer and send the information to a web panel or to an email address that has been set up by the individual deploying the keylogger. FBI Agents have identified a YouTube video containing a tutorial on how to use the Limitless Keylogger version 8.1.3, to include newer versions. An individual with a male voice, who identified himself as "Mephobia," provided over sixteen minutes of instruction on how to create the keylogger file and view the keystrokes of the infected computer. This individual entered the username "Mephobia" and password when explaining how to set up a personal web panel to view the keystroke logs of the infected computer. During the tutorial, "Mephobia" showed viewers how to "spoof" the extension (technique used to masquerade or hide the true extension such as .doc, .pdf, or .exe or others in order to mislead the victim/user of the infected computer) of the keylogger file (to trick the victim into clicking an email attachment which would install the keylogger), and how to generate a fake message when the logger is executed on the infected computer. When "Mephobia" provided instructions on how to use the startup editor, "Mephobia" gave the following instruction:

> …startup editor I suggest that you enable this if you want to keep the victims keep logging the victims if you don't want to keep logging the victims and um you just want

> them to get logged until they restart don't check this this will make it so when they restart their computer the server will start up again…

14. The Limitless Keylogger executable kit includes a feature to crypt the keylogger executable so that it is "fully undetectable" by anti-virus tools. "Mephobia" provided instructions on how to crypt the keylogger in the same YouTube.com video mentioned above. Based on my training and experience, crypting the executable obfuscates the malware so that it does not resemble the piece of code that was detected as malicious by anti-virus software. Additionally, the Limitless Keylogger and Syndicate Stealer were offered for sale on a forum called Hackforums.net dedicated mostly to hacking and other online criminal activity.

15. In an article entitled "Attackers Use Keyloggers, Email to Steal Data in 'NightHunter' Attacks" that was posted on the website securityweek.com, a security firm discovered that attackers have been stealing Google, Yahoo, Facebook, Skype, Dropbox, Amazon, Yahoo, Hotmail, LinkedIn, Rediff and banking credentials from a wide range of organizations, including sectors like energy, health, insurance, education, and even charities. According to that article, cybercriminals distribute the malware with the aid of phishing emails that appear to be related to purchase orders, payments, jobs and inquiries. Many malicious keyloggers involved in these attacks were identified. The security firm told SecurityWeek that victims may have been spotted in various countries, including the United States, Saudi Arabia, the United Kingdom, India and Malaysia. The article also stated the following:

> The phishing emails contain an archive file that in most cases hides a keylogger. Several such threats have been identified in this campaign, including Limitless Logger Lite, Predator Pain, Spyrex, Aux Logger, Neptune, Mr. Clyde Logger, Ultimate Logger, Syslogger and Syndicate Logger.

Based on my experience with this investigation, it appears the article was referring to same Limitless Keylogger and Syndicate Stealer malware referenced in this affidavit.

16. "Mephobia" was an active member on a forum called Hackforums.net, a forum where a member can obtain hacking tools and programs and chat with other members on the forum. According to information observed on Hackforums.net in February 2015, the user known as "Mephobia" was 19 years old and joined forum on January 22, 2011. Information on the forum further revealed "Mephobia" last visited the forum on January 13, 2014 and posted approximately 5,392 messages.

17. A review of the Hackforums.net forum revealed that on June 18, 2012, "Mephobia" posted a message entitled "…{free} REFLECT LOGGER {Limitless Logger Trial} {NOOB FRIENDLY} {WORKING} {FUD}…" which advertised the availability of a keylogger named REFLECT LOGGER for free for members of the forum. Based on the title of the posting, this keylogger may be related to the Limitless Keylogger. The acronym FUD is most likely stands for "fully undetectable" as further described in paragraphs 14 and 21. The message further contained "…PLEASE LEAVE A THANKS OR A VOUCH FOR THIS! I WORKED ON THIS AND TOOK MY TIME TO MAKE A FREE KEYLOGGER FOR YOU GUYS!..."

18. According to records obtained from PayPal, the account HFMephobia@gmail.com is registered to the following individual:

Registration Information
First Name: Zachary
Last Name: Shames
CC Statement Name: Limitless
Email: HFMephobia@gmail.com, jackhillen95@gmail.com
Account number: 1414938196128858417

FBI Agents confirmed that this PayPal account was created on February 21, 2011, and has, between July 2012 through at least July 2014, received many payments in the increments of $20, $25, $30, $35, and $40. The total amount of money received in this account was in the thousands of dollars. The activity log revealed that the email address jackhillen95@gmail.com was used many times to log into this PayPal account.

19. During this investigation, the email address HFMephobia@gmail.com was identified as being linked to "Mephobia." The subscriber information for HFMephobia@gmail.com revealed that the email account was subscribed to "Mephobia HF" with the recovery (or secondary back-up) e-mail as zlshames@gmail.com.

20. The historical usage records for HFMephobia@gmail.com revealed the following:

a. Many users of the Limitless Keylogger communicated via email with the individual utilizing the email address HFMephobia@gmail.com.

b. The email account HFMephobia@gmail.com was used to received PayPal payments from the users of the keylogger.

c. The individual who utilized the email account HFMephobia@gmail.com received many emails from the email account admin@limitlessproducts.org.

d. The individuals who utilized email accounts HFMephobia@gmail.com and jkbest22@gmail.com communicated with each other many times over email.

e. The individual who utilized the email account zlshames@gmail.com sent an email to HFMephobia@gmail.com, which contained information where the email was originating from, such as the full path about the server and script that was associated with sending this email. The X-PHP-Script was limitlessproducts.org/sqltest/frontend/demo-contacts-process.php and the X-Source-Dir was limitlessproducts.org:/public_html/sqltest/frontend.

21. Review of the email account HFMephobia@gmail.com revealed that the account holder responded to questions posed by individuals who have either purchased the keyloggers or were seeking to purchase them. For those individuals who have expressed interest in purchasing the Limitless Keylogger, the account holder directed them to the website limitlessproducts.org. Examples of these emails are as follows:

a. On July 19, 2012, an individual at keygp@live.com emailed HFMephobia@gmail.com wanting to know the difference between a keylogger and a RAT: "Does the RAT automatically include the features from the Keylogger? Include the PINLogger? Or is it simply a client holder which would be used to download these files to their computer individually." In my training and experience and in the context of the email between keygp@live.com and HFMephobia@gmail.com, the acronym RAT stands for either a Remote Access Tool or Remote Access Trojan, allowing a user to remotely spy on and control another electronic device. In response, the account holder of HFMephobia@gmail.com provided a link to the Limitless executable and gave the explanation: "The rat lets you download and execute whenever you want. you can also view their desktop, and do much more. It does not however have all the features the keylogger does though. And mine works. I just helped a bunch of people use it. if you want help. add me on Skype: Mephobia.HF"

b. On April 16, 2013, the account holder of eduardosantos@loja-auto.com emailed HFMephobia@gmail.com complaining about two limitations of the Limitless Keylogger: "…I bought the limitless logger yesterday. First impression is that it works great. Anyway, I found two major upsets… - its not fud right now. I crypt with it's crypter and infinity crypter and detections are high. When AVG detects I, personally in Portugal, I'm fucked as everybody in into AVG…Will make it fud soon? – I have a critical problem with the characters of the victims pc…" Based on other emails between HFMephobia@gmail.com and other users, the acronym FUD stands for "fully undetectable." In response, the account holder of HFMephobia@gmail.com defended his product: "I know it is. And by the way, if you are crypting with infinity crypter then it is not the Logger's fault its not FUD. That would be a crypter problem. Not a keylogger ones. I do not believe it supports accent marks It has the ability to detect if the letters are in Unicode, which it did, but I do not think it allows accent marks as far as I know. I'll see what I can do." In a subsequent email to eduardosantos@loja-auto.com, the account holder of HFMephobia@gmail.com was adamant that the keylogger was not the problem because he developed it: "Trust me. I made this logger. I coded it. It doesn't change the way the words are typed…It just records what they type."

c. On July 12, 2014, the account holder of donex_p@rocketmail.com emailed HFMephobia@gmail.com to ask if the Limitless Keylogger could collect data from a Firefox browser and if the logger would be updated with that specific function. The account holder of HFMephobia@gmail.com response was simply "no." In response, the account holder of donex_p@rocketmail.com asked if HFMephobia@gmail.com knew of other loggers besides Syndicate. The account holder of HFMephobia@gmail.com responded "No. Syndicate or Limitless is all I know."

22. According to the business records of HostGator, which provided web hosting services for the domain name limitlessproducts.org, the username "mephobia" and domain name "limitlessproducts.org" were registered to the following individual:

First Name: Zachary
Last Name: Shames
Email Address: hfmephobia@gmail.com
Address: 872 Forestville Meadows Drive
City: Great Falls
State: VA

According to information received from HostGator, the above account and domain name was suspended due to phishing content issue. HostGator personnel advised the account holder of limitlessproducts.org had received keylogger data and that the customer associated with the username "mephobia" and domain name "limitlessproducts.org" was keylogging a large volume of material.

A preliminary review of data/records received from HostGator revealed the computer server which hosted the domain name limitlessproducts.org contained numerous computer files which contain what appears to be keystroke data taken from victims' computers.

ACCESS FROM JAMES MADISON UNIVERITY

23. Based on records from Google, the account HFMephobia@gmail.com was registered to the following individual:

Name: Mephobia HF
Recovery email: zlshames@gmail.com

Based of publicly available Internet records, a number of IP addresses which accessed this account were registered to JMU.

24. Based on records from Google, the account jackhillen95@gmail.com was registered to the following individual:

Name: Jack Hillen
Recovery email: hfmephobia@gmail.com

Based on publicly available Internet records, a number of IP addresses which accessed this account were also registered to JMU.

25. Based on records from Google, the account zlshames@gmail.com was registered to the following individual:

Name: Zach Shames
Recovery email: hfmephobia@gmail.com

Based of publicly available Internet records, a number of IP addresses which accessed this account were also registered to JMU.

26. Based on records received from JMU, the IP addresses which accessed the PayPal account associated with HFMephobia@gmail.com, at the relevant dates and times

during the periods from April 14, 2014 to September 25, 2014, were registered to the following account:

Name: ZACHARY LEE SHAMES
Email: shameszl@dukes.jmu.edu

According to JMU records, the above account accessed JMU computer networks from devices including the following:

Device/Host Name: Zachs-iPhone
Device MAC address: 38:f:4a:57:98:69

Device/Host Name: ZachsVAIO
Client: Microsoft Windows 8 / Server 2012
Device MAC address: 80:1f:02:dc:6f:81

According to JMU records, the above account, using the above listed devices, accessed JMU computer networks, from various locations at the university including Shenandoah Hall, a dormitory.

27. A review of the email account HFMephobia@gmail.com revealed that messages were sent to this account from a device named ZachsVAIO and IP addresses registered to JMU. A review of this email account further revealed that on or about February 19, 2014, it received an email from an account named limitlesskeystrokemonitor@gmail.com entitled "Aux Logger – You got Logs! – PC:ZACHSVAIO". The body of the email contained what appeared to be a screenshot of a computer screen associated with the following computer:

Computer Name: ZachsVAIO
Username: Zach
Operating System: Microsoft Windows 8.1

Based on the review of the above email, it appears the individual who utilized the account HFMephobia@gmail.com received a screenshot of his own computer screen which based on my experience, could be a test of the functions of the Limitless Keylogger malware. VAIO is a line of computers sold by the Sony Corporation. Sony VAIO computers have both laptop and desktop models.

28. A review of the email account HFMephobia@gmail.com revealed email messages originating from an iPhone device and IP addresses registered to JMU, which were sent from this account discussing the Limitless Keylogger.

29. According to records received from JMU, ZACHARY LEE SHAMES is a student at JMU and residing at SUBJECT PREMISES. SHAMES listed 872 Forestville Meadows Drive, Great Falls, Virginia as his home residence. JMU listed August 25, 2014, as the first day of class for the 2014-2015 academic year. Based on information detailed in paragraph 26, it appears SHAMES' JMU account continued to access the PayPal account associated with HFMephobia@gmail.com in the current academic year.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

30. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. 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 Rule 41(e)(2)(B).

31. *Probable cause.* 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."

32. *Forensic evidence.* 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 establishes how 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. As explained herein, information stored within a computer and other electronic storage media 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, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contains information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

b. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

c. 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.

d. 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.

e. 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.

33. *Necessity of seizing* or *copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review 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:

e. 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 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.

f. 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.

g. 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.

h. Because several people may share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

34. Based on the aforementioned information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations, or attempted violation, of Title 18, United States Code, Sections 1030 (computer fraud), 1343 (wire fraud), 371 (conspiracy), and 2 (aiding and abetting) may be located at SUBJECT PREMISES and on the person of ZACHARY LEE SHAMES, as further described in Attachment A. I request that the Court issue the proposed search warrant for the SUBJECT PREMISES and person of ZACHARY LEE SHAMES to search for items described in Attachment B.

Respectfully submitted,

Peter M.D. Vu
Special Agent, Federal Bureau of Investigation

Subscribed and sworn to before me on March 16, 2015

The Honorable Joel C. Hoppe
United States Magistrate Judge

Reviewed by Alexander T.H. Nguyen
Assistant United States Attorney, Eastern District of Virginia

IN THE
UNITED STATES DISTRICT COURT
FOR THE
WESTERN DISTRICT OF VIRGINIA
HARRISONBURG DIVISION

IN THE MATTER OF THE SEARCH OF THE PREMISES LOCATED AT JAMES MADISON UNIVERSITY, SHENANDOAH HALL ROOM B305, 1671 CARRIER DRIVE, HARRISONBURG, VIRGINIA 22807, AND THE PERSON OF ZACHARY LEE SHAMES	Case No. **Filed Under Seal**

ATTACHMENT A

Person To Be Searched

Zachary Lee Shames, who was born on August 18, 1995, and resides at SUBJECT PREMISES James Madison University, Shenandoah Hall Room B305, 1671 Carrier Drive, Harrisonburg, Virginia 22807.

Descriptive information for Zachary Lee Shames:

Social Security Number: 102-84-6325
Race: White
Gender: Male
Height: 5’7”
Weight: 143 lbs
Hair Color: Black
Eye Color: Brown

IN THE
UNITED STATES DISTRICT COURT
FOR THE
WESTERN DISTRICT OF VIRGINIA
HARRISONBURG DIVISION

IN THE MATTER OF THE SEARCH OF THE PREMISES LOCATED AT JAMES MADISON UNIVERSITY, SHENANDOAH HALL ROOM B305, 1671 CARRIER DRIVE, HARRISONBURG, VIRGINIA 22807, AND THE PERSON OF ZACHARY LEE SHAMES	Case No. **<u>Filed Under Seal</u>**

ATTACHMENT B

Items To Be Seized

The items to be seized are evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1030 (computer fraud), 1343 (wire fraud), 371 (conspiracy), and 2 (aiding and abetting) pertaining to the following matters:

a. Records relating to malware executables;

b. Records relating to the dissemination of malicious and fraudulent software;

c. Records relating to configuration files and commands for infected computers;

d. Records relating to instant messaging;

e. Records relating to the purchase or leasing of, or payment for, computer infrastructure and computer peripherals;

f. Records relating to online and business revenues

g. Records and information relating to the use of any botnets, Trojans, personal identifying information related to any online fraud schemes;

h. Records and information relating to the Limitless Keylogger, Syndicate Stealer/Keylogger, and keylogger malware;

i. Records and information relating to any associates and customers who have either used or purchased the keylogger;

j. Records related to any wire transfers, including to PayPal and other online payment providers;

k. Records and information relating to who created, used, or communicated with the account, including records about their identities and whereabouts;

l. Computer with the following description (Make: Sony, Model: Vaio);

m. Cellular telephone device with the following description (Make: Apple, Model: iPhone);

n. Records of user names, encryption keys, and passwords to secure communication services;

o. Records of personal and business activities relating to the operation and ownership of computer systems, such as telephone records, notes, books, diaries, and reference materials;

p. Records pertaining to accounts held with Internet Service Providers or of Internet use;

q. Records pertaining to accounts help with telephone service providers or of telephone use, including cellular telephones;

r. As used above, the terms records, documents, programs, applications or materials include records, documents, programs, applications or materials created, modified or stored in any form.

s. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

1. evidence of who used, owned, or controlled the COMPUTER 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, and correspondence;

2. evidence of software that would allow others to control the COMPUTER, 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;

3. evidence of the lack of such malicious software;

4. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

5. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

6. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

7. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

8. evidence of the times the COMPUTER was used;

9. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

10. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

11. records of or information about Internet Protocol addresses used by the COMPUTER;

12. records of 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;

13. contextual information necessary to understand the evidence described in this attachment.

t. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, 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); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

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.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.