ZA:SK
F. #2015R00439

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

15M 769

- - - - - - - - - - - - - - - - X

UNITED STATES OF AMERICA

- against -

FABIO GASPERINI,

Defendant.

- - - - - - - - - - - - - - - - X

TO BE FILED UNDER SEAL

COMPLAINT AND AFFIDAVIT IN SUPPORT OF APPLICATION FOR ARREST WARRANT

(18 U.S.C. § 1030(a)(4))

EASTERN DISTRICT OF NEW YORK, SS:

GEORGE SCHULTZEL, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation, duly appointed according to law and acting as such.

In or about and between December 2014 and August 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant FABIO GASPERINI, together with others, did knowingly and with intent to defraud access a protected computer without authorization and exceed authorized access, and by means of such conduct further the intended fraud and obtain a thing of value.

(Title 18, United States Code, Section 1030(a)(4))

The source of your deponent's information and the grounds for his belief are as follows:[1]

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been employed by the FBI since July 2010. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for financial fraud and cybercrime. These investigations are conducted both in an undercover and overt capacity. I have participated in investigations involving search warrants and arrest warrants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

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: (a) my personal participation in this investigation, (b) reports made to me by other law enforcement authorities, and (c) information obtained from confidential sources of information.

3. Since approximately December 2014, the FBI has been conducting an investigation into the unlawful accessing of computer servers in the United States and abroad.

4. The government's investigation has uncovered evidence supporting a conclusion that the defendant FABIO GASPERINI has surreptitiously gained entry into multiple servers in the United States and abroad that he did not have permission to access, including servers in the Eastern District of New York. Furthermore, the evidence obtained in

---

[1] Because the purpose of this Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

the investigation supports a conclusion that GASPERINI has used that unauthorized access to further a scheme to defraud for his own financial gain and worked with others to carry out the scheme and to launder the proceeds of the scheme.

5. Specifically, the evidence described below demonstrates that the defendant gained unauthorized access to network and file servers belonging to others and then installed malicious software on those servers that he used to perpetrate, among other schemes, a "click fraud," described more fully in paragraph 10. The defendant fraudulently obtained money for advertisers -- as payment for advertisements that had not actually been viewed or clicked by potential customers -- as a result of those schemes.

The Offense Conduct

6. On or about December 5, 2014, a confidential source working with the FBI ("CS-1")[2] observed a network of computers that had been infected with malicious software. The computers in the network were primarily Network Attached Storage devices ("Servers") and the malicious software targeted additional such Servers for infection and addition to the network. Such Servers are typically used as a centralized resource for large-scale data storage and transfer and can serve various functions including as file servers, cloud-based servers, and file transfer protocol servers.

7. CS-1 observed the malicious code that was targeting Servers within his custody and control. The malicious software's infection of Servers included the following steps, among others: accessing the Servers without permission; adding an administrative user

[2] CS-1's information has been corroborated by independent evidence, including observations by law enforcement.

account named "request" with a password of "ciaociao"[3]; taking measures to ensure that others could not access the Servers through the same manner; and downloading and executing electronic files to further expand the network to other Servers.

8. As described infra, the investigation revealed that the malicious software at issue had been installed on the Servers by the defendant FABIO GASPERINI.

9. One of the electronic files downloaded by the malicious software was the file "http://185.14.30.79/SOO.sh" (the "SOO Propagation Script").[4] The SOO Propagation Script facilitated the infection of the Servers and the identification of additional servers for infection. CS-1 observed the SOO Propagation Script on or about December 8, 2014. A search of publicly available information indicated that the host of the SOO Propagation Script (http://185.14.30.79) was a host server with domain name "gaspolo.uaservers.net". CS-1 also observed that the server pushing the SOO Propagation Script originated from the Internet Protocol ("IP") address 94.40.91.149, based in Italy.[5]

10. The SOO Propagation Script contained two additional scripts including http://23.231.6.11/emme (the "EMME Script"). The EMME Script attempted to fake internet traffic metrics for ads appearing on a website identified herein as the "Target Website." Specifically, CS-1 observed the EMME Script repeatedly issuing commands that would effect a "click" on an ad appearing on the Target Website. Based on my knowledge, training, and experience, such commands are typically used to further "click fraud," by which individuals fraudulently obtain money from advertisers -- who pay for their ads on a per-click basis -- by

---

[3] The password is the Italian word "ciao" repeated twice.

[4] A script is a list of commands that can be executed without user interaction.

[5] An IP address is a numerical label assigned to each device participating in a computer network.

simulating actual clicks on website ads through an automated computer program. Advertisers who are victims of click fraud end up paying for clicks perpetrated by automated software rather than clicks completed by actual potential customers interested in the advertisers' products. Here, based on open-source reporting, the click fraud appears to be against website ads placed by a company ("Victim 1"), among others.

11. According to CS-1, the EMME Script, when active, downloads a particular "user-agent string"[6] that it employs as part of the click fraud scheme described above. The user-agent string can help identify the individual who designed the malicious script. Here, the EMME Script downloads the user-agent string from the IP address 178.79.183.247, which is the IP address associated with a virtual server operated by a virtual private server provider based in Galloway, New Jersey (the "NJ Server"). Records obtained from that service provider revealed that the customer using the NJ Server is the defendant FABIO GASPERINI, who resides in Rome, Italy.

12. A search of publicly available databases revealed that the registration information for the Target Website included a registration email sent from an email address identified herein as the "Target Email Address." Records obtained from Google revealed that the subscriber name for the Target Email Address was FABIO GASPERINI.

13. A search of publicly available information for "Fabio Gasperini" revealed a November 15, 2009 Facebook.com posting authored by Fabio Gasperini promoting his (now defunct) website http://www.gaspolo.it. A search of publicly available information indicated

---

[6] A user-agent is typically used by a software agent such as a web browser to identify itself, its application type, operating system, software vendor or software revision, by submitting a characteristic identification string to its operating peer.

that the domain name "gaspolo.it" was registered to "Fabio Gasperini" at the address "Via Dei Frassini 132" in Rome, Italy, from November 2009 to November 2011. As discussed supra in paragraph 9, the server that hosted the SOO Propagation Script had the domain name "gaspolo.uaservers.net".

14. A search of publicly available information for "Gasperini Via Dei Frassini 132" revealed additional domain names associated with that address, including "fashionist.info" and "incucina.info". A search of publicly available information indicated that each domain name was registered to "Fabio Gasperini" with a registration email of the Target Email Address.

15. On March 26, 2015, United States Magistrate Judge Marilyn D. Go of the Eastern District of New York issued a search warrant for the Target Email Address. During the execution of the search warrant, law enforcement agents observed email communications and other records which appear to confirm that the Target Email Address is, indeed, used by an individual named FABIO GASPERINI who resides in Rome, Italy.

16. For example, law enforcement agents observed digital photographs of an Italian identification card in the name of FABIO GASPERINI, listing a date of birth of November 30, 1982, and an address of "Via Dei Frassini N.132" in Rome, Italy, and bearing a photograph. Law enforcement agents also observed email communications in which GASPERINI used the Target Email Address to send and receive communications regarding: (i) the purchase, activation, and registration of domain names, websites, and servers associated with the SOO Propagation Script and the Target Website; and (ii) payments resulting from online pay-per-click advertising on the Target Website and other websites registered to

GASPERINI. The communications regarding servers included billing and other notifications related to the maintenance of the NJ Server.

17. The communications regarding payments included email communications from GASPERINI to other individuals in which GASPERINI forwarded payment notifications -- images of documents that confirm payments by Victim 1 in connection with the click fraud described above -- and included instructions on how to redeem the payments.

18. Law enforcement agents also observed several electronic files related to the click fraud stored within the storage space associated with the Target Email Address, which files included a propagation script similar to the SOO Propagation Script, and digital photographs of computer screens showing computer code directing "clicks" against Victim 1's ads.

WHEREFORE, your deponent respectfully requests that an arrest warrant be issued for the defendant FABIO GASPERINI, so that he be dealt with according to law. I further request that this affidavit and the arrest warrant be filed under seal as these documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and disclosure of these documents would give the targets of the investigation an opportunity to destroy evidence, harm or threaten victims or other witnesses, change patterns of behavior, notify confederates, and flee from or evade prosecution.

GEORGE SCHULTZEL
Special Agent, Federal Bureau of Investigation

Sworn to before me this
14th day of August, 2015

S/ Lois Bloom

THE HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK