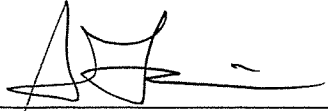


12 MAG 2984

Approved:   
SARAH Y. LAI  
Assistant United States Attorney

Before: THE HONORABLE  
United States Magistrate Judge  
Southern District of New York

----- x

UNITED STATES OF AMERICA	:	<u>SEALED COMPLAINT</u>
- v. -	:	Violations of 18 U.S.C. §§ 1030(b) and 1349
MIHAI IONUT PAUNESCU, a/k/a "Virus,"	:	COUNTY OF OFFENSE: NEW YORK
Defendant	:	

----- x

SOUTHERN DISTRICT OF NEW YORK, ss.:

M. KATHRYN SCOTT, being duly sworn, deposes and says that she is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE

(Conspiracy to Commit Computer Intrusion)

1. From at least in or about 2005, up to and including in or about November 2012, in the Southern District of New York and elsewhere, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit computer intrusion offenses in violation of Title 18, United States Code, Sections 1030(a)(2), (a)(4), (a)(5)(A) and (a)(6), to wit, PAUNESCU knowingly would and did provide critical online infrastructure that was used to control and/or receive stolen information from computers infected with malicious software ("malware"), including malware intentionally designed to steal bank account access information, launch distributed denial of service ("DDoS") attacks, and send unsolicited junk electronic mail ("email").

2. It was a part and an object of the conspiracy that MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, and others

known and unknown, would and did intentionally access computers without authorization, and thereby would and did obtain information from protected computers, for purposes of commercial advantage and private financial gain, and in furtherance of criminal and tortious acts in violation of the Constitution and the laws of the United States, and the value of the information obtained would and did exceed \$5,000, in violation of Title 18, United States Code, Section 1030(a)(2).

3. It was a further part and an object of the conspiracy that MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, and others known and unknown, willfully, knowingly, and with intent to defraud, would and did access protected computers without authorization, and by means of such conduct would and did further the intended fraud and obtain anything of value, in violation of Title 18, United States Code, Section 1030(a)(4).

4. It was a further part and an object of the conspiracy that MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, and others known and unknown, willfully and knowingly would and did cause the transmission of a program, information, code, and command, and as a result of such conduct, would and did intentionally cause damage without authorization, to protected computers, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

5. It was a further part and an object of the conspiracy that MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, and others known and unknown, in transactions affecting interstate and foreign commerce, and computers used by and for the Government of the United States, willfully, knowingly, and with intent to defraud, trafficked in passwords and similar information through which computers may be accessed without authorization, in violation of Title 18, United States Code, Section 1030(a)(6).

#### Overt Acts

6. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. By at least in or about October 2010, a computer belonging to a business located in Manhattan, New York, had been infected with malicious software known as the "Gozi

Virus," and login credentials for online banking had been stolen from that computer.

b. Beginning in or about March 2012, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, rented a dedicated server located in California which functioned as a proxy server (the "Paunescu Proxy Server") for computers infected with the Gozi Virus and malware known as the Zeus Trojan.

c. On or about June 11, 2012, a computer located in New York, New York, contacted the Paunescu Proxy Server.

d. At various times from at least in or about May 2012, up to and including at least in or about August 2012, certain computers belonging to and used by the United States National Aeronautics and Space Administration ("NASA") that had been infected with the Gozi Virus contacted the Paunescu Proxy Server.

e. In or about February 2012, over \$200,000 was fraudulently transferred out of a bank account controlled by a victim ("Victim-1") whose computer had been infected with the Gozi Virus.

(Title 18, United States Code, Sections 1030(b),  
(c) (2) (B) and (c) (4) (B).)

#### COUNT TWO

(Conspiracy to Commit Bank Fraud)

7. From at least in or about 2005, up to and including in or about November 2012, in the Southern District of New York and elsewhere, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit bank fraud, in violation of Title 18, United States Code, Section 1344, to wit, PAUNESCU knowingly would and did provide critical online infrastructure that was used to spread malware designed to steal login information for bank accounts in the United States and elsewhere, and to receive such stolen data which was then used to transfer funds from the victims' accounts without their authorization.

8. It was a part and an object of the conspiracy that MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, and others known and unknown, willfully and knowingly would and did execute a scheme and artifice to defraud a financial institution, the

accounts and deposits of which were then insured by the Federal Deposit Insurance Corporation ("FDIC"), and to obtain moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, a financial institution, by means of false and fraudulent pretenses, representations, and promises, in violation of Title 18, United States Code, Section 1344.

#### Overt Acts

9. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. By at least in or about October 2010, a computer belonging to a business located in Manhattan, New York, had been infected with the Gozi Virus, and login credentials for online banking had been subsequently stolen from that computer.

b. Beginning in or about March 2012, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, rented the Paunescu Proxy Server.

c. On or about June 11, 2012, a computer located in New York, New York, contacted the Paunescu Proxy Server.

d. At various times from at least in or about May 2012, up to and including at least in or about August 2012, certain NASA computers infected with the Gozi Virus contacted the Paunescu Proxy Server.

e. In or about February 2012, over \$200,000 was fraudulently transferred out of a bank account controlled by Victim-1 whose computer had been infected with the Gozi Virus.

(Title 18, United States Code, Section 1349.)

#### COUNT THREE

(Conspiracy to Commit Wire Fraud)

10. From at least in or about 2005, up to and including in or about November 2012, in the Southern District of New York and elsewhere, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit wire fraud, in violation of Title 18, United

States Code, Section 1343, to wit, PAUNESCU knowingly would and did provide critical online infrastructure that was used to control and/or receive stolen data from computers infected with malware that was intentionally designed, among other things, to steal bank account access information, launch DDoS attacks, and distribute spam.

11. It was a part and an object of the conspiracy that MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, and others known and unknown, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, willfully and knowingly would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343.

#### Overt Acts

12. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere.

a. By at least in or about October 2010, a computer belonging to a business located in Manhattan, New York, had been infected with the Gozi Virus, and login credentials for online banking had been stolen from that computer.

b. Beginning in or about March 2012, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, rented the Paunescu Proxy Server.

c. On or about June 11, 2012, a computer located in New York, New York, contacted the Paunescu Proxy Server.

d. At various times from at least in or about May 2012, up to and including at least in or about August 2012, certain NASA computers infected with the Gozi Virus contacted the Paunescu Proxy Server.

e. In or about February 2012, over \$200,000 was fraudulently transferred out of a bank account controlled by Victim-1 whose computer had been infected with the Gozi Virus.

(Title 18, United States Code, Section 1349.)

The bases for my knowledge and the foregoing charges are, in part, as follows:

13. I am a Special Agent with the FBI. I am currently assigned to the Computer Intrusion Squad of the New York Division of the FBI, and have received training in computer technology, computer fraud, intellectual property crimes, and white collar crimes. Prior to joining the FBI, I worked for approximately five years as an electrical engineer in the private sector designing computer hardware and software. I am familiar with the facts and circumstances set forth below from my personal participation in the investigation, including my examination of reports and records, interviews I have conducted, and conversations with other law enforcement officers and other individuals. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, unless noted otherwise.

#### DEFINITIONS

14. Based on my training and experience, I am aware of the following:

a. "Bulletproof hosting" is the practice of knowingly providing computers, IP addresses, domains and related technical services to cyber criminals and shielding those clients from detection by law enforcement authorities and others concerned with Internet security. Bulletproof hosts generally lease servers and IP addresses from legitimate web hosting providers, then sublease those facilities to customers who are cyber criminals. By acting as a go-between, the bulletproof hosts limit the amount of visibility a legitimate host may have into the illegal activities of the ultimate sublessee.

b. "Malware," short for "malicious software," is computer software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to describe a variety of hostile or intrusive program code. Computer viruses, trojans, and spyware are types of malware.

c. A "trojan" is malware that appears to perform a desirable function for the user prior to running or installing but instead facilitates the unauthorized access of the user's computer system.

d. A "botnet" is a group of Internet-connected computers whose security defenses have been secretly breached with malware. Botnets are typically controlled by one computer called a command and control server. Each compromised computer is known as a "bot." The owner of the command and control server can direct the botnet to, among other things, send bank account login information, distribute spam, operate as proxies (blindly forwarding Internet data), or participate in other cybercrime.

e. A "distributed denial of service," or "DDoS," attack occurs when botnets are used to target a single system. The targeted system is inundated with external communication requests from a botnet controlled by hackers such that it becomes unable to respond to legitimate Internet traffic or its response time is significantly slowed.

f. A "server" is a centralized computer that provides services for other computers connected to it via a network or the Internet. For example, a server that is configured so that its sole task is to support a World Wide Web site is known simply as a "Web server." Similarly, a server that only stores and processes email is known as a "mail server." The computers that use the server's services are sometimes called "clients." When a user accesses email, Internet web pages, or files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client's computer via the network or Internet.

g. A "proxy" is a computer that acts as a "middleman" for a user making indirect connections to other network services. A client computer connects to a proxy and instructs it to connect to another computer. The destination computer perceives an incoming connection from the proxy, not the client computer. Like many network services, proxies have legitimate uses, but they are often used by cyber criminals to conceal their identity and location.

h. An "Internet Protocol address," or IP address, is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods. Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination.

i. An "Internet Service Provider," or ISP, is a commercial service that provides Internet connections for its

subscribers. ISPs may also provide Internet email accounts and other services unique to each particular ISP.

#### OVERVIEW OF PAUNESCU'S CRIMINAL SCHEMES

15. Based on my review of electronic interceptions, searches of servers, subscriber and registration information for a cellphone, servers and IP addresses, and documents prepared by other agents and private sector network security experts, and as set forth more fully below, there is probable cause to believe that MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, a Romanian national residing in Bucharest, was a so-called "bulletproof host" who knowingly provided critical online infrastructure, namely, servers, IP addresses and domains, that enabled cyber criminals throughout the world to distribute viruses and other malware, to control and receive information from computers infected with such malware, to launch DDoS attacks, and/or to distribute spam. PAUNESCU facilitated the deployment of destructive viruses and other malware including the Gozi Virus, the Zeus Trojan, SpyEye, and BlackEnergy. In total, the cybercrime schemes that PAUNESCU has supported with his online infrastructure have caused tens of millions of dollars in losses and affected well over one million computers in countries throughout the world.

#### The Gozi Virus

16. Since in or about 2010, I have been personally involved in the investigation of the Gozi Virus. Based on my investigation, including my interviews with a distributor of the Gozi Virus<sup>1</sup> and my communications with other law enforcement agents, I know that the design of the Virus began in or about 2005, and its distribution began in or about 2007. The Gozi Virus was spread by, among other means, concealing it within apparently benign document files or websites. When a victim opened the document or visited the website, the Gozi Virus was secretly installed onto the victim's computer, where it remained virtually undetectable by antivirus software. Once installed, the Gozi Virus collected data from the infected computer in order to capture the victim's account user name, password and other

---

<sup>1</sup> The distributor has been arrested and has pleaded guilty to various fraud and computer intrusion charges. The distributor has cooperated with U.S. law enforcement officials in hopes of receiving a reduced sentence. The distributor's information has proven reliable and has been largely corroborated by independent evidence.



vital security information, and sent that data to a computer server controlled by co-conspirators, who used the data to transfer funds fraudulently out of the victim's account and, ultimately, into their personal possession. In the past, the co-conspirators used the Gozi Virus primarily to target accounts at European banks. Beginning in or about 2010, they began using the Virus to attack U.S. bank accounts, including FDIC-insured bank accounts at a large financial institution headquartered in Manhattan, New York. Since its inception, the Gozi Virus has infected, at a minimum, over a million computers around the world, including at least 40,000 in the United States, and has caused at least millions of dollars in losses.

### The Zeus Trojan

17. I have communicated with other FBI agents who have investigated the Zeus Trojan. Based on those communications and my own review of reports about the Zeus Trojan prepared by private sector network security experts, I know that, similar to the Gozi Virus, the Zeus Trojan was designed to steal computer access data, such as user names and passwords, for, among other things, bank accounts, email accounts, and social networking websites. Like the Gozi Virus, the Zeus Trojan typically infected a victim's computer when the victim clicked on a link, or opened a file, that was attached to a seemingly legitimate email message, but which was actually an email message sent by computer hackers for the purpose of infecting the victim's computer. Once installed, the Zeus Trojan allowed computer hackers to secretly monitor the victim's computer activity, recording, among other things, the victim's bank account numbers, passwords, and authentication information as they were typed by the victim into the infected computer to access online banking websites, among other things. The stolen bank account data was then used to transfer funds fraudulently out of the victim's accounts.

### SpyEye

18. I am also aware from my communications with, and review of documents prepared by, another FBI agent who has investigated SpyEye that it is similar to Gozi and Zeus. SpyEye is malware intentionally designed to facilitate unauthorized access to the computers of individuals, businesses and other entities in order to steal online banking credentials, credit card information and other personal identification information. The information is then fraudulently used to withdraw money from victims' accounts or to make purchases of goods and services.

## BlackEnergy

19. Based on my communications with another FBI agent and my review of reports prepared by that agent as well as by private sector network security experts, I am aware that BlackEnergy is malware that launches World Wide Web-based DDoS attacks. Updated versions of BlackEnergy use additional programming to extend the malware's functionality beyond DDoS attacks to include, for example, gathering account access credentials and sending spam. Hackers have used BlackEnergy botnets to target, among others, political entities, financial institutions and commercial enterprises, including numerous e-commerce sites operated by businesses in the United States.

### THIS INVESTIGATION

#### I. Identification of MIHAI IONUT PAUNESCU as A Bulletproof Host and His Computer Infrastructure

20. As explained in detail below, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, was identified as a bulletproof host as a result of the interception of a cellphone that he used and the search of certain computers and a domain that he operated, in furtherance of his illegal activities. The evidence showed that PAUNESCU knowingly provided critical online infrastructure to co-conspirators involved with, among other malware, the Gozi Virus, the Zeus Trojan, SpyEye and BlackEnergy, as well as the distribution of spam.

##### A. Interception of the Paunescu Cellphone

21. I have communicated with members of the Romanian Police's Directorate for Combating Organized Crime ("DCCO"), who are conducting their own investigation of MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant. I have also reviewed reports that they prepared. Based on those communications and reports, I am aware that between on or about March 16, 2012 and on or about June 29, 2012,<sup>2</sup> the DCCO conducted court-authorized surveillance of communications over a cellphone with a call number ending in 441, believed to be PAUNESCU's cellphone (the "Paunescu Cellphone"), and obtained subscriber records for that phone. I have reviewed the wiretap evidence and the subscriber information, which were provided to the FBI pursuant to a Mutual Legal Treaty Assistance request. The subscriber information

---

<sup>2</sup> Interception was temporarily suspended from April 12 to 24, 2012.

showed that the Paunescu Cellphone is registered to a company named KLM Internet & Gaming SRL ("Internet & Gaming"). Publicly available records showed that Internet & Gaming was initially registered to PAUNESCU in or about February 2010, but the registrant's name has since changed. Nevertheless, intercepted messages demonstrated that PAUNESCU was, in fact, the person using the Paunescu Cellphone. For example:<sup>3</sup>

a. On or about March 27, 2012, the user of the Paunescu Cellphone placed a call to Romanian Commercial Bank to inquire about procedures for withdrawing \$20,000. During the call, the user of the Cellphone identified himself as "Mihai Ionut Paunescu" and provided his personal identification number (*Cod Numeric Personal* or CNP) as a certain number ending in 019 (the "019 CNP"). The *Cod Numeric Personal* is the equivalent of a national identification number. Passport information for PAUNESCU shows that the 019 CNP is PAUNESCU's CNP.

b. On or about March 29, 2012, the user of the Paunescu Cellphone sent a text message to an unidentified male ("UM"), provided the UM with the name "Paunescu Mihai Ionut" and the 019 CNP, and instructed the UM to call a certain telephone number and "say that you are the contract holder (i.e. me)[.]"

c. On or about April 1, 2012, the user of the Paunescu Cellphone sent a text message which read, "answer me, damn it, I'm Virus." On or about April 2, 2012, an unidentified male called PAUNESCU and addressed him as "Virus." As discussed in paragraph 23(d) below, "Virus" is a nickname that PAUNESCU used.

22. From my review of English translations of the intercepted communications over the Paunescu Cellphone, I also learned the following:

a. MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, used the Cellphone to access what appeared to be status pages (written in English) for various servers. Each status page contained multiple fields, including the IP address

---

<sup>3</sup> The original text messages and phone conversations were in the Romanian language. Excepted where otherwise indicated, this affidavit provides preliminary English translations by a translator contracted to the FBI. Where necessary, I have provided my interpretations of certain words/terms in brackets, which are based on my training, experience and participation in this investigation.

of the server, the sell price, the payment method, and one entitled "Server For." For example, PAUNESCU accessed a status page for the server assigned IP address 93.114.43.18. In the field "Server For:" was written "malware 100%SBL." (SBL likely stands for Spamhaus Block List. Spamhaus is a not-for-profit organization that tracks IP addresses found to be used for distributing spam or malware. It maintains various lists of untrustworthy IP addresses which are referred to generally as the Spamhaus Block List (or SBL). The interceptions revealed that several times a month, PAUNESCU monitored the Spamhaus list at <http://www.spamhaus.org/sbl/latest/>, which listed the IP addresses and domains most recently added to and removed from the Spamhaus Block List.) The server status page also displayed a "Buy Price" of "114EU" and a "Sell Price" of "330EU" for the server, suggesting that PAUNESCU was charging his customer three times the amount he himself was paying for the server. As another example, PAUNESCU accessed a status page for the server assigned IP address 109.163.227.85. The "Server For:" field read "dns 100%SBL." The "Sell Price" for this server was "5020EU." These intercepts showed that PAUNESCU was knowingly providing web hosting services to cyber criminals.

b. PAUNESCU also received many automated status messages about numerous servers, identified by their IP addresses. These messages generally alerted PAUNESCU to when a system "dropped" or "is back." The IP addresses he tracked in this manner included an IP address that received stolen data forwarded from the Paunescu Proxy Server (discussed in paragraph 26(b)(ii) below), the 109.163.227.85 IP address discussed in subparagraph (a) above, and many others that appeared on a password-protected domain named "Adminpanel.ro," which described numerous servers associated with malware and spam, as discussed in the next section.

c. Based on the fact that PAUNESCU was accessing status pages for servers described as hosting malware and/or blocked by Spamhaus, was receiving automated messages regarding the operational status of servers that were connected to malware, and was listing buy and sell prices for those servers, I believe that he had control over and knew the content of those servers, and was running a bulletproof hosting scheme.

## **B. Search of Adminpanel.ro**

23. The Paunescu Cellphone was a smartphone capable of connecting to the Internet. DCCO officials observed the Cellphone being used to access the domain Adminpanel.ro, with the user name "admin" and the password "mi[portion of password

redacted]ru" on multiple occasions between in or about March 2012, and in or about June 2012. Publicly available records showed that Adminpanel.ro was hosted at IP address 89.37.59.85. On or about May 7, 2012, the DCCO searched the domain Adminpanel.ro, pursuant to a Romanian court order. I have reviewed the search results, which were provided by the Romanian authorities pursuant to a Mutual Legal Assistance request, and observed the following:

a. Adminpanel.ro contained several data tables. One data table, entitled "vm" [which likely stands for virtual machine],<sup>4</sup> contained information about approximately 130 physical servers, including an identification number for the customer using each server, the server name, the type of processor in the server, and the "buyprice" for the server. That data table also contained a column entitled "for," which provided a brief description (in English) of the contents hosted on the server, including: "spy [meaning SpyEye]/malware," "100%SBLmalware," "ilegal [sic]," "semi-legal non sbl," "facebook spam 0%SBL," and "zeus 100%SBL." In fact, by their descriptions, approximately half of the approximately 130 servers listed in this data table contained malware, was on the Spamhaus Block List, and/or was being monitored to determine if they were added to the Spamhaus Block List. These descriptions and monitoring activity provide further cause to believe that PAUNESCU knew his customers were involved with malware, including the Zeus and SpyEye Trojans.

b. The "vm" table included the IP addresses 64.62.146.67 to 64.62.146.99 and 64.62.146.100 to 64.62.146.126, which were assigned to the Paunescu Proxy Server, which PAUNESCU had leased from an ISP located in California (the "California ISP"). As discussed in paragraphs 24 to 26 below, computers infected with the Gozi Virus and the Zeus Trojan had communicated with several of the IP addresses within these ranges. Tellingly, the "vm" data table described the content hosted at these IP addresses as "100%SBL," which I understand to mean that these IP addresses all appeared on the Spamhaus Block List.

---

<sup>4</sup> Based on my training, experience and communications with other agents, I am aware that in hosting web servers, database administrators often set up "virtual machines," in which a single server computer is configured to run software to emulate multiple computer systems. It is advantageous for web hosts to do so because they can host several customers on a single machine, with each customer having access to what appears to be its own computer with the appropriate software to meet its needs.

c. As discussed in paragraph 22(a) above, PAUNESCU had used the Paunescu Cellphone to access the status pages for servers assigned IP addresses 93.114.43.18 and 109.163.227.85, respectively. These IP addresses also appeared in the "vm" data table in Adminpanel.ro, and the descriptions of their contents (in the "for" column) were exactly the same as appeared on the status pages (in the "Server For" field). Accordingly, I believe that the status pages in fact contained data from Adminpanel.ro, and that PAUNESCU, who signed in as "admin," had access to all of the information in that domain.

d. Another data table in Adminpanel.ro, entitled "user," contained a list of nicknames and their associated email addresses, among other information. The first entry was "admin" and was associated with the email address tech@powerhost.ro. As noted above, PAUNESCU had used the user name "admin" to log in to Adminpanel.ro. The fourth entry was "personal" and associated with the email address virus@powerhost.ro. As discussed above, PAUNESCU had texted "I'm Virus," while using the Paunescu Cellphone. Given that PAUNESCU is Virus, the identification of the virus@powerhost.ro email address on Adminpanel.ro as a "personal" email address further supports the conclusion that the person who controlled Adminpanel.ro was PAUNESCU.

e. In addition, I recognize several of the other nicknames in the "user" table based on my own investigation of the Gozi conspiracy and my communications with other FBI agents. One of the nicknames ("Nickname-1") belonged to another bulletproof host, who was described by a Gozi co-conspirator as an individual who provided servers "for botnets/Spyware/Malware/Adware/Codecs/Exploits/Pharma/Trojans/Anti-Spyware/Drop Project/TDS, etc high risk content."<sup>5</sup> A second nickname ("Nickname-2") had an email address that had been used as the abuse-complaints email for a computer that was either a command and control server or proxy server for a Gozi botnet. Notably, the "vm" data table described the content of four of the servers leased to Nickname-2 as "malware," "semilegal," "fake av [meaning antivirus] 100%SBL," and "100%SBL," respectively. A third nickname had appeared on an Internet forum used by cyber criminals, offering to sell SpyEye.

---

<sup>5</sup> This description was included in an instant message stored on a private communications server used by members of the Gozi conspiracy. The server was searched pursuant to a warrant issued by the Honorable Debra Freeman, United States Magistrate Judge for the Southern District of New York, in or about late October 2010.

## II. Specific Examples of Servers Controlled by PAUNESCU

### A. A Botnets Proxy Server

24. Another FBI agent and I have communicated several times with a special agent of NASA's Office of the Inspector General (the "NASA-OIG Agent"), and learned that from on or about December 14, 2007, to on or about August 9, 2012, approximately 190 NASA computers had been infected with the Gozi Virus. On several occasions between on or about May 8, 2012, and on or about August 9, 2012, Gozi-infected NASA computers sent data to IP address 64.62.146.101 without the computer user's authorization. The extracted data included login credentials for an eBay account and a NASA email account, details of websites visited, and even contents of Google chat messages.

25. The NASA-OIG Agent has also communicated with a malware researcher at a respected university in the United States (the "Researcher") who has assisted with other cybercrime investigations and whose information has proven to be reliable in the past. The Researcher maintained a database containing malware infections, the IP addresses of servers which the compromised computers contacted after becoming infected, and the dates of such contacts. That database contained the following information:

a. A computer infected with malware known as the "Virus" virus had attempted to communicate with IP address 64.62.146.93 on or about August 18, 2012; and

b. Between on or about May 27, 2012, and on or about August 17, 2012, at least seven computers infected with "Zbot" (another name for the Zeus Trojan) had attempted to communicate with seven different IP addresses: 64.62.146.90, 64.62.146.85, 64.62.146.83, 64.62.146.82, 64.62.146.81, 64.62.146.76, and 64.62.146.71.

26. Based on publicly available records, I learned that the IP addresses discussed in paragraphs 24 and 25 were assigned to the Paunescu Proxy Server. Subscriber records and historical connection logs maintained by the California ISP which rented out the Proxy Server, provided pursuant to a court order, further revealed that:

a. "Paunescu Mihai Ionut," with a physical address in Bucharest, Romania, and the email address of "paunescu@powerhost.ro," was the subscriber of the Paunescu Proxy Server;

b. During the periods covered by the historical connection logs - from on or about May 29, 2012, to on or about June 12, 2012, and from on or about June 22, 2012, to on or about July 6, 2012:

i. Over 25,000 unique IP addresses had connected to IP address 64.62.146.101 on the Paunescu Proxy Server, including approximately 20,000 located in the United States. Among them were the IP address of the Gozi-infected NASA computer that sent details of visited websites on or about June 5, 2012, as well as at least three IP addresses assigned to computers located in Manhattan, New York.

ii. In addition to IP address 64.62.146.101, the Paunescu Proxy Server also had other IP addresses within the 64.62.146.64/26 block which received incoming Internet traffic. The Proxy Server was configured to automatically route all incoming traffic from the 64.62.146.64 to 64.62.146.127 block of IP addresses out through IP address 184.105.224.250, and then to IP address 93.114.44.27, which was registered to an ISP/telecommunications company in Romania (the "Romanian ISP").

iii. I know from my training, experience and communications with other cyber investigators that within the source code or a configuration file of most malware is a list of IP addresses and/or domain names with which the infected computer is directed to communicate. This programming practice, together with the fact that all traffic going to the 64.62.146.64 to .127 IP address range was automatically routed to the same IP address at the Romanian ISP, provide probable cause to believe that the 25,000 IP addresses which contacted the Paunescu Proxy Server did so because they were infected with malware that specifically directed them to the Proxy Server.

#### **B. A Botnet Command and Control Server**

27. I have also spoken with and reviewed documents prepared by an FBI Agent who was involved in the investigation of the BlackEnergy botnet, and learned that as of on or about June 2, 2011, a command and control domain for the BlackEnergy botnet was hosted at IP address 86.55.210.101. This IP address had been used to launch DDoS attacks against numerous businesses in the United States and elsewhere from on or about May 17, 2011, through on or about June 22, 2011. IP address 86.55.210.101 falls within the IP address block 86.55.210.0 to 86.55.211.255. Publicly available records showed that as of June 2, 2011, this entire block of IP addresses was registered to a Romanian company named SC KLM Invest COM SRL ("KLM Invest"), with an address at



"Str. Elena Doamna Nr. 4, Com. Afumati, Jud. Ilfov." According to the DCCO, this is the address of the mother of MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant. The contact person for KLM Invest was PAUNESCU. Accordingly, I believe that PAUNESCU was also providing web hosting services for members of the BlackEnergy conspiracy. Registration records for this block of IP addresses had not changed as of on or about November 9, 2012.

28. Other agents and I have examined a command and control server for a Gozi botnet that was seized in the Netherlands pursuant to a Mutual Legal Assistance Treaty request (the "Dutch Gozi C&C Server"), in or about October 2010. The analysis revealed that this Server had communicated with over a million compromised computers worldwide. The information transmitted from the compromised computers to the Dutch Gozi C&C Server included most compromised computers' language setting. Because approximately 22,000 of the compromised computers used the "en-US" language setting, which I believe stands for American English, I believe that approximately 22,000 of the compromised computers which connected to the Dutch Gozi C&C Server were located in the United States. At least one of those 22,000 computers belonged to, and was located at, a business in Manhattan, New York. Another agent has analyzed that compromised computer and saw that it contained remnants of the Gozi Virus, which antivirus software had attempted to remove, but which remained identifiable as the Gozi Virus based on certain signature characteristics. The bank account user name and password of the person who used the compromised computer were found to be stored on the Dutch Gozi C&C Server, along with at least 3,000 other user names for accounts at approximately seven U.S. banks, including banks headquartered in Manhattan, New York, the deposits of which were insured by the FDIC. Accordingly, I believe that the banking user names found on the Dutch Gozi C&C Server had been stolen from compromised computers infected with the Gozi Virus.

29. Finally, I have communicated with or reviewed reports by agents who have conducted forensic analyses of two Gozi-infected computers, and compared the dates of infection to the dates of subsequent fraudulent transfers from the victims' accounts, and know that those two victims alone sustained an aggregate of over \$6 million in losses. I have also spoken with and reviewed reports prepared by other agents involved in the Zeus investigation. I learned that based on searches of instant messaging and command-and-control servers, analysis of

compromised computers, and victim interviews, they concluded that the Zeus Trojan has caused tens of millions of dollars in losses.

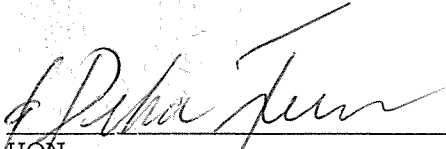
WHEREFORE, deponent prays that an arrest warrant be issued for the above-named defendant, and that he be imprisoned or bailed, as the case may be.



\_\_\_\_\_  
M. KATHRYN SCOTT  
Special Agent  
Federal Bureau of Investigation

NOV 19 2012

Sworn to before me this  
\_\_\_\_\_th day of November, 2012



\_\_\_\_\_  
HON.  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF NEW YORK

Debra Freeman  
United States Magistrate Judge  
Southern District of New York