ORIGINAL

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
- - - - - - - - - - - - - - - - - - - -X

UNITED STATES OF AMERICA : **SEALED INDICTMENT**

-v.- : 13 Cr.

MIHAI IONUT PAUNESCU, : **13 CRIM 041**
a/k/a "Virus,"

Defendant. :

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

COUNT ONE

(Conspiracy to Commit Computer Intrusion)

The Grand Jury charges:

THE DEFENDANT

1. At all times relevant to this Indictment, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, was a Romanian national residing in Bucharest, Romania.

OVERVIEW OF THE DEFENDANT'S CRIMINAL SCHEME

2. As set forth more fully below, at all times relevant to this Indictment, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, operated a so-called "bulletproof hosting" service using computers in Romania, the United States, and elsewhere. Through this service, PAUNESCU, like other bulletproof hosts, knowingly provided critical online infrastructure to cyber criminals that allowed them to commit online criminal activity with little fear of detection by law enforcement. Among other things, in exchange for fees, PAUNESCU provided cyber criminals

JUDGE PATTERSON

with Internet Protocol ("IP") addresses and servers in a manner designed to enable them to preserve their anonymity and evade detection by law enforcement.

3. Through his bulletproof hosting service and as set forth in greater detail below, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, knowingly facilitated and aided a number of online cyber crimes relating to:

a. Malicious software (or "malware"): PAUNESCU's bulletproof hosting service facilitated the distribution of malware including "banking Trojans" such as the "Gozi Virus," the "Zeus Trojan," and the "SpyEye Trojan." Banking trojans enable cyber criminals to steal the bank account information of unsuspecting victims, and the banking Trojans PAUNESCU aided others in proliferating have, since their inception, caused tens of millions of dollars in losses worldwide.

b. Distributed denial of service ("DDoS") attacks: PAUNESCU's bulletproof hosting service enabled cyber criminals to initiate and execute DDoS attacks, including through a type of malware commonly referred to as "BlackEnergy."

c. Spam: PAUNESCU's bulletproof hosting service enabled cyber criminals to transmit spam e-mail over the Internet.

OVERVIEW OF RELEVANT CYBER CRIMES

Banking Trojans

4. Banking Trojans are typically designed to steal personal information, such as usernames and passwords, needed to access online accounts, including online bank accounts. Banking Trojan malware is often concealed within seemingly harmless documents or webpages which, in turn, are typically contained within unsolicited electronic mail messages (or "spam") from apparently benign senders. When a victim opens the document or visits the webpage, the banking Trojan malware is secretly installed onto the victim's computer.

5. Once installed, the malware steals user names, passwords and other security information and forwards these data to a so-called "command-and-control" server controlled by cyber criminals, who then use the information to steal money from victims' online bank accounts. Banking Trojan malware can be tailored by cyber criminals to steal online banking credentials for specific banks.

6. The banking Trojan commonly known as the Gozi Virus was first developed beginning in or about 2005 and distributed over the Internet beginning in or about 2007. Law enforcement officers first observed the Zeus Trojan online in or about 2007 and the SpyEye Trojan in or about 2009. By itself, the Gozi Virus has infected over one million victim computers

worldwide, including at least 40,000 victim computers in the United States, as well as computers in Germany, Great Britain, Poland, France, Finland, Italy, Turkey and elsewhere. Collectively, the Gozi Virus, the Zeus Trojan and the SpyEye Trojan have infected millions of computers around the world; targeted numerous banks in the United States and elsewhere, including at least one major United States bank headquartered in Manhattan, New York; and caused at least tens of millions of dollars in losses.

DDoS Attacks and BlackEnergy Malware

7. In a DDoS attack, cyber criminals typically use a "botnet" - a large number of computers connected to the Internet - to bombard a victim's computer system or web server with bogus requests for information, causing the computer system or website to cease functioning temporarily. Cyber criminals typically create botnets by infecting victim computers with malware that allows the cyber criminals to control each computer, or "bot," secretly and without the computer user's knowledge or authorization. A botnet may consist of thousands or even millions of infected computers. Cyber criminals typically control botnets using command-and-control servers, through which they send individual bots instructions, including instructions to engage in DDoS attacks. Bot malware can also be configured to perform other functions, such as stealing information from

infected computers, in a manner similar to banking Trojans, or transmitting spam e-mails.

8. "BlackEnergy" is the name commonly given to a particular piece of bot malware that was initially designed to launch DDoS attacks. Cyber criminals have used botnets created by computers infected with BlackEnergy to launch DDoS attacks against computer systems used by, among others, political entities, financial institutions and commercial enterprises, including numerous e-commerce sites operated by businesses in the United States and elsewhere. Subsequent versions of BlackEnergy have been modified to engage in criminal activity besides DDoS attacks, including stealing account access credentials from victims' computers and causing those computers to transmit spam.

Spam

9. "Spam" is unsolicited bulk e-mail that is transmitted over the Internet in a manner that hides the true source of the spam and the identity of the cyber criminals who send it ("spammers"). As noted above, spam is often a means by which cyber criminals distribute malware over the Internet, including banking Trojans and bot malware. Spammers typically take steps to conceal the true origin of their spam e-mail messages not only to hide their identity but also to defeat certain Internet e-mail filters that might otherwise be set to block e-mail identified as being generated by a particular

source, permitting the spam to reach the greatest number of recipients. Among the means that spammers use to hide their identities and the true source of the spam are bots and servers located at bulletproof hosting services.

THE DEFENDANT'S BULLETPROOF HOSTING SERVICE

10. At various times relevant to this Indictment, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, provided critical online infrastructure and Internet services to his criminal clients and co-conspirators and did so in a manner that enabled them to perpetrate their online criminal schemes and to shield themselves from their victims and law enforcement.

11. Among other things, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant:

a. Rented servers and IP addresses from legitimate Internet service providers ("ISPs") and then re-rented them to cyber criminals;

b. Provided to his clients servers that, among other things, operated as command-and-control servers for botnets and other illegal activity or functioned as so-called "proxies," that is, servers that acted as online intermediaries between victim computers and the ultimate recipients, thereby allowing cyber criminals to shield their true identities and locations.

c. Monitored the IP addresses that he controlled to determine if they appeared on a special list of suspicious or

untrustworthy IP addresses maintained by the Spamhaus Project ("Spamhaus"), a non-profit organization whose mission is to, among other things, track the sources of spam on the Internet, and whose "Spamhaus Block List" contains IP addresses that administrators at legitimate Internet service providers often consult when determining whether to block access to their networks from Internet traffic, including e-mails, originating from certain IP addresses; and

d. Relocated his customers' data to different networks and IP addresses, including networks and IP addresses in other countries, to avoid being blocked as a result of Spamhaus or law enforcement scrutiny.

STATUTORY ALLEGATIONS

12. From at least in or about 2011, 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, including servers and IP addresses, to assist criminals engaging in unlawful online schemes.

13. 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, Sections 1030(a)(2) and (c)(2)(B).

14. 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).

15. 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).

16. 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

17. 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. From in or about late 2011 through at least in or about mid-2012, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, and/or his co-conspirators not named as defendants herein caused approximately 60 computers belonging to the National Aeronautics and Space Administration ("NASA") to be infected with the Gozi Virus, resulting in approximately $19,000 in losses to NASA.

b. In or about May 2011, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, provided a server through a company he controlled that acted as a command-and-control server for a BlackEnergy botnet.

c. Beginning in or about March 2012, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, rented a server from an ISP in California which he and/or his co-conspirators not named as defendants herein subsequently configured to function as a proxy server for computers infected with the Gozi Virus and the Zeus Trojan (the "Paunescu Proxy Server").

d. On or about June 4, 2012, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, and/or co-conspirators not named as defendants herein caused a computer located at a bank in Manhattan, New York, to contact the Paunescu Proxy Server.

e. In or about May 2012, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, and/or co-conspirators not named as defendants herein caused a NASA computer infected with the Gozi Virus to send login credentials for an eBay account to the Paunescu Proxy Server without the NASA computer user's knowledge or consent.

f. At various times from at least in or about May 2012 through in or about November 2012, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, maintained a database which

described certain servers that he controlled or leased as being used for, among other things, "spyeye 100%SBL," "zeus 100%SBL," "100%sbl, phising [sic]," "100%SBL malware," and "fake av [antivirus] 100%SBL."

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

COUNT TWO

(Conspiracy to Commit Bank Fraud)

18. The allegations contained in paragraphs 1 through 11 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

19. From at least in or about 2011, 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 support malware designed to steal account access information for bank accounts in the United States and elsewhere.

20. 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

21. 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 co-conspirator had caused a computer belonging to a business located in Manhattan, New York, to be 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, which he and/or his co-conspirators subsequently configured to operate as a proxy server for computers infected with the Gozi Virus and the Zeus Trojan.

c. On or about June 4, 2012, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, and/or co-conspirators

not named as defendants herein caused a computer located at a bank in Manhattan, New York, to contact the Paunescu Proxy Server.

d. In or about May 2012, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, and/or co-conspirators not named as defendants herein caused a NASA computer infected with the Gozi Virus to send login credentials for an eBay account to the Paunescu Proxy Server without the computer user's knowledge or consent.

e. At various times from at least in or about May 2012 through in or about November 2012, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, maintained a database which described certain servers that he controlled or leased as being used for "spyeye 100%SBL," "zeus 100%SBL," "100%sbl, phising [sic]," "100%SBL malware," and "fake av [antivirus] 100%SBL."

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

COUNT THREE

(Conspiracy to Commit Wire Fraud)

The Grand Jury further charges:

22. The allegations contained in paragraphs 1 through 11 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

23. From at least in or about 2011, 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, including servers and IP addresses, to assist criminals engaging in unlawful online schemes.

24. 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

25. 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 co-conspirator had caused a computer belonging to a business located in Manhattan, New York, to be 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, which he and/or his co-conspirators not named as defendants herein subsequently configured to operate as a proxy server for computers infected with the Gozi Virus and the Zeus Trojan.

c. On or about June 4, 2012, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, and/or co-conspirators not named as defendants herein caused a computer located at a bank in Manhattan, New York, to contact the Paunescu Proxy Server.

d. In or about May 2012, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, and/or co-conspirators not named as defendants herein caused a NASA computer infected with the Gozi Virus to send login credentials for an eBay account to the Paunescu Proxy Server without the computer user's knowledge or consent.

e. At various times from at least in or about May 2012 through in or about November 2012, PAUNESCU maintained a

database which described certain servers that he controlled or leased as being used for "spyeye 100%SBL," "zeus 100%SBL," "100%sbl, phising [sic]," "100%SBL malware," and "fake av [antivirus] 100%SBL."

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

FORFEITURE ALLEGATION AS TO COUNT ONE

26. As a result of committing the computer intrusion conspiracy offense alleged in Count One of this Indictment, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, shall forfeit to the United States,

a. pursuant to 18 U.S.C. § 982(a)(2)(B), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of the offense charged in Count One; and

b. pursuant to 18 U.S.C. § 1029(c)(1)(C), any personal property used or intended to be used to commit the offense charged in Count One.

Substitute Assets Provision

27. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States, pursuant to 18 U.S.C. § 982(b), to seek forfeiture of any other property of the defendant up to the value of the above-described forfeitable property.

(Title 18, United States Code, Sections 982 and 1030, and Title 21, United States Code, Section 853.)

FORFEITURE ALLEGATIONS AS TO COUNTS TWO AND THREE

28. As a result of committing the bank fraud conspiracy offense alleged in Count Two and/or the wire fraud conspiracy offense alleged in Count Three of this Indictment, MIHAI IONUT PAUNESCU, a/k/a "Virus," the defendant, shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461, all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of the offenses charged in Counts Two and Three.

Substitute Assets Provision

29. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States, pursuant to 18 U.S.C. § 982(b), to seek forfeiture of any other property of the defendant up to the value of the above-described forfeitable property.

(Title 18, United States Code, Sections 981, 1029, 1343, 1344, and 1349; Title 28, United States Code, Section 2461; and Title 21, United States Code, Section 853.)

FOREPERSON

PREET BHARARA
United States Attorney

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

MIHAI IONUT PAUNESCU,
a/k/a "Virus,"

Defendant.

SEALED INDICTMENT

13 Cr.

(18 U.S.C. §§ 1030(b) and 1349)

PREET BHARARA
United States Attorney.

A TRUE BILL

Foreperson.

1/17/13 - Filed Sealed Indictment.
Judge Fox
U.S.M.J.