UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

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

UNITED STATES OF AMERICA	:	INFORMATION
-v.-	:	11 Cr. 387 (LBS)
NIKITA KUZMIN,	:	
Defendant.	:	

- - - - - - - - - - - - - - - - - - - -x

COUNT ONE

(Bank Fraud Conspiracy)

The United States Attorney charges:

INTRODUCTION

1. From at least in or about 2005, up to and including in or about November 2010, in the Southern District of New York and elsewhere, NIKITA KUZMIN, the defendant, and others known and unknown, stole bank account information from the computers of individuals and businesses in the United States and around the world using malicious computer code, known as "Gozi" (the "Gozi Virus"). KUZMIN and his co-conspirators used that stolen information to access the bank accounts of at least tens of thousands of individuals and businesses without the victims' knowledge or authorization, and then to steal money from those bank accounts for KUZMIN's and his co-conspirators' personal use.

2. Since its inception, the Gozi Virus has infected, at a minimum, over 100,000 computers around the world, including at least 25,000 computers in the United States, and has caused,

at a minimum, tens of millions of dollars in losses.

BACKGROUND

3. The Gozi Virus was named by private sector information security experts in the United States who, in or about 2007, discovered that a previously unrecognized malicious computer code was stealing personal bank account information (such as account numbers, usernames, and passwords) from computers across Europe on a vast scale, while remaining virtually undetectable in the computers it infected. The Gozi Virus was later spread to the United States.

4. The Gozi Virus was distributed and delivered to victims' computers in different ways. In one method, the virus was disguised as an apparently-benign .pdf document (i.e., a document in the widely used .pdf format, which is easily shared among different computer operating systems). When a victim clicked on the .pdf document, the Gozi Virus was secretly downloaded onto the victim's computer, where it was generally undetectable by anti-virus software. Once downloaded, the Gozi Virus collected data from the infected computer in order to capture the victim's bank account user name, password, and other vital security information, and sent that data to a computer server controlled by certain users of the Gozi Virus, who used the data fraudulently to transfer funds out of the victim's account and, ultimately, into their personal possession.

5. At all times relevant to this Information, NIKITA KUZMIN, the defendant, was a citizen and resident of Russia with training and expertise in computer science. As set forth in greater detail below, at all times relevant to this Information, KUZMIN was the chief architect and promoter of the Gozi Virus.

THE SCHEME TO DEFRAUD

6. Beginning in or about 2005, NIKITA KUZMIN, the defendant, began to design the Gozi Virus to steal the personal bank account information of individuals and businesses on a widespread basis, which information he and others could then use to obtain money from those bank accounts. KUZMIN created a list of technical specifications for the Gozi Virus, and hired a sophisticated computer programmer ("CC-1") to write the virus's "source code," the unique computer programming language enabling the virus to operate. After months of work, CC-1 completed work on the source code for the Gozi Virus, and provided it to KUZMIN.

7. Thereafter, as part of the fraudulent scheme, in or about 2006, NIKITA KUZMIN, the defendant, among other things began providing the Gozi Virus to co-conspirators on a rental basis for a weekly fee through an operation he termed "76 Service." In particular, through "76 Service," KUZMIN enabled co-conspirators, on their own, to configure the Gozi Virus to steal varying types of data (for example, passwords, usernames, or other pieces of information), and to launch the Gozi Virus to

attack others' computers, causing those computers to send the stolen data to a particular computer server controlled by KUZMIN. For a weekly fee, KUZMIN provided each co-conspirator with access to the specific data stolen as a result of that particular co-conspirator's use of the virus. Kuzmin advertised "76 Service" on one or more Internet forums devoted to cybercrime and other criminal activities.

8. In or about 2008, following various operational and technical difficulties, among other things, NIKITA KUZMIN, the defendant, ceased renting the Gozi Virus through "76 Service." Thereafter, in or about 2009, KUZMIN was approached by various co-conspirators who sought to acquire the source code for the Gozi Virus. Among these co-conspirators were a group of individuals who sought to use the Gozi Virus to attack computers and steal money from bank accounts in the United States on a widespread basis (the "U.S.-Facing CCs"), as well as individuals who sought to use the Gozi Virus for similar purposes in particular European countries.

9. As a further part of the fraudulent scheme, from in or about 2009 until in or about mid-2010, NIKITA KUZMIN, the defendant, sold the Gozi Virus source code to various co-conspirators, including, but not limited to, the U.S.-Facing CCs, and another particular co-conspirator ("CC-2"), for at least approximately $50,000 per sale plus a guaranteed share of future

profits from the co-conspirators' use of the virus.

10. As a further part of the fraudulent scheme, in or about 2009, CC-2 became "partners" with NIKITA KUZMIN, the defendant, in the promotion of the Gozi Virus, working with KUZMIN to, among other things, sell the Gozi Virus source code and/or rent the Gozi Virus to co-conspirators, and to arrange for sophisticated computer programmers periodically to refine and update the Gozi Virus in order to ensure, among other things, that the virus remained virtually undetectable in victims' computers.

STATUTORY ALLEGATIONS

11. From at least in or about 2005, up to and including in or about November 2010, in the Southern District of New York and elsewhere, NIKITA KUZMIN, the defendant, and others known and unknown, unlawfully, willfully, and knowingly did combine, conspire, confederate, and agree together and with each other to commit an offense against the United States, to wit, to violate Section 1344 of Title 18, United States Code.

12. It was a part and an object of the conspiracy that NIKITA KUZMIN, the defendant, and others known and unknown, unlawfully, willfully, and knowingly, would and did execute, and attempt to execute, a scheme and artifice to defraud financial institutions, the accounts and deposits of which were then insured by the Federal Deposit Insurance Corporation, and to

obtain moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, such financial institutions, by means of false and fraudulent pretenses, representations, and promises, in violation of Title 18, United States Code, Section 1344.

OVERT ACTS

13. 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. On or about October 30, 2009, NIKITA KUZMIN, the defendant, sent an instant message communication to a co-conspirator about bank accounts.

b. On or about January 9, 2010, KUZMIN offered to provide a co-conspirator with access to the Gozi Virus.

c. On or about August 13, 2010, $8,710 was transferred out of the bank account of a victim in Bronx, New York ("Victim-1") without Victim-1's consent after Victim-1's bank account information was stolen from a computer infected with the Gozi Virus.

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

COUNT TWO

(Bank Fraud)

The United States Attorney further charges:

14. The allegations contained in paragraphs 1 through 10 and 13 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

15. From at least in or about 2005, up to and including in or about November 2010, in the Southern District of New York and elsewhere, NIKITA KUZMIN, the defendant, unlawfully, willfully, and knowingly did execute, and attempt to execute, a scheme and artifice to defraud financial institutions, namely, Citibank and other banks, the accounts and deposits of which were then insured by the Federal Deposit Insurance Corporation, and to obtain the moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, such financial institutions, by means of false and fraudulent pretenses, representations, and promises, to wit, using the computer virus known and described as the "Gozi Virus," and working with others, KUZMIN accessed and attempted to access without authorization computers owned by private individuals and businesses, and thereby obtained and attempted to obtain bank account access information of such individuals and businesses, which information was used fraudulently to withdraw millions of dollars from such individuals' and businesses' bank accounts.

(Title 18, United States Code, Sections 1344 & 2.)

COUNT THREE

(Access Device Fraud Conspiracy)

The United States Attorney further charges:

16. The allegations contained in paragraphs 1 through 10 and 13 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

17. From at least in or about 2005, up to and including in or about November 2010, in the Southern District of New York and elsewhere, NIKITA KUZMIN, the defendant, and others known and unknown, unlawfully, willfully, and knowingly did combine, conspire, confederate, and agree together and with each other to commit offenses against the United States, to wit, to violate Sections 1029(a)(2), 1029(a)(3), 1029(a)(5), and 1029(a)(6) of Title 18, United States Code.

18. It was a part and an object of the conspiracy that NIKITA KUZMIN, the defendant, and others known and unknown, unlawfully, willfully, and knowingly, and with intent to defraud, as part of an offense affecting interstate and foreign commerce, would and did traffic in and use one and more unauthorized access devices during any one-year period, and by such conduct did obtain anything of value aggregating $1000 and more during that period, in violation of Title 18, United States Code, Section 1029(a)(2).

19. It was further a part and an object of the conspiracy that NIKITA KUZMIN, the defendant, and others known and unknown, unlawfully, willfully, and knowingly, and with intent to defraud, as part of an offense affecting interstate and foreign commerce, would and did possess fifteen and more devices which were counterfeit or unauthorized access devices, in violation of Title 18, United States Code, Section 1029(a)(3).

20. It was further a part and an object of the conspiracy that NIKITA KUZMIN, the defendant, and others known and unknown, unlawfully, willfully, and knowingly, and with intent to defraud, as part of an offense affecting interstate and foreign commerce, would and did effect and attempt to effect transactions, with one and more access devices issued to another person and persons, to receive payment and any other thing of value during any 1-year period, the aggregate value of which is equal to and greater than $1,000, in violation of Title 18, United States Code, Section 1029(a)(5).

21. It was further a part and an object of the conspiracy that NIKITA KUZMIN, the defendant, and others known and unknown, unlawfully, willfully, and knowingly, and with intent to defraud, as part of an offense affecting interstate and foreign commerce, would and did solicit a person for the purpose of offering an access device, without the authorization of the

issuer of the access device, in violation of Title 18, United States Code, Section 1029(a)(6).

OVERT ACTS

22. In furtherance of the conspiracy and to effect the illegal objects thereof, the overt acts listed in paragraph 13 (a)-(c) above, among others, were committed in the Southern District of New York and elsewhere.

(Title 18, United States Code, Section 1029(b)(2).)

COUNT FOUR

(Access Device Fraud)

The United States Attorney further charges:

23. The allegations contained in paragraphs 1 through 10 and 13 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

24. From at least in or about 2005, up to and including in or about November 2010, in the Southern District of New York and elsewhere, NIKITA KUZMIN, the defendant, unlawfully, willfully, and knowingly, and with intent to defraud, as part of an offense affecting interstate and foreign commerce, did effect and attempt to effect transactions, with one and more access devices issued to another person and persons, to receive payment and any other thing of value during any 1-year period, the aggregate value of which is equal to and greater than $1,000, to wit, using the computer virus known and described as the "Gozi

Virus," and working with others, KUZMIN accessed and attempted to access without authorization computers owned by private individuals and businesses, and thereby obtained and attempted to obtain bank account access information of such individuals and businesses, which information was used fraudulently to withdraw millions of dollars from such individuals' and businesses' bank accounts.

(Title 18, United States Code, Sections 1029(a)(5), 1029(b)(1), 1029(c)(1)(A)(ii), and 2.)

COUNT FIVE

(Conspiracy to Commit Computer Intrusion)

The United States Attorney further charges:

25. The allegations contained in paragraphs 1 through 10 and 13 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

26. From at least in or about 2005, up to and including in or about November 2010, in the Southern District of New York and elsewhere, NIKITA KUZMIN, the defendant, and others known and unknown, unlawfully, willfully, and knowingly did combine, conspire, confederate, and agree together and with each other to commit offenses against the United States, to wit, to violate Title 18, United States Code, Sections 1030(a)(2), 1030(a)(4).

27. It was a part and an object of the conspiracy that NIKITA KUZMIN, the defendant, and others known and unknown, unlawfully, willfully and knowingly, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, intentionally accessed a computer without authorization, and thereby obtained and attempted to obtain information contained in a financial record of a financial institution, and of a card issuer as defined in 15 U.S.C. § 1602(n), and from a protected computer, the value of which exceeded $5,000, in violation of Title 18, United States Code, Section 1030(a)(2).

28. It was further a part and an object of the conspiracy that NIKITA KUZMIN, the defendant, and others known and unknown, knowingly and with intent to defraud, accessed and attempted to access a protected computer without authorization, and by means of such conduct furthered the intended fraud and obtained something of value exceeding $5,000, in violation of Title 18, United States Code, Section 1030(a)(4).

OVERT ACTS

29. In furtherance of the conspiracy and to effect the illegal objects thereof, the overt acts listed in paragraph 13 (a)-(c) above, among others, were committed in the Southern District of New York and elsewhere.

(Title 18, United States Code, Section 1030(b).)

COUNT SIX

(Computer Intrusion Obtaining Information)

The United States Attorney further charges:

30. The allegations contained in paragraphs 1 through 10 and 13 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

31. From at least in or about 2005, up to and including in or about November 2010, in the Southern District of New York and elsewhere, NIKITA KUZMIN, the defendant, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, intentionally accessed and attempted to access a computer without authorization, and thereby obtained and attempted to obtain information contained in a financial record of a financial institution, and of a card issuer as defined in 15 U.S.C. § 1602(n), and from a protected computer, the value of which exceeded $5,000, to wit, using malicious computer code known and described as the "Gozi Virus," and working with others, KUZMIN accessed and attempted to access without authorization computers owned by private individuals and businesses, and thereby obtained and attempted to obtain bank account access information of such individuals and businesses, which information was used

fraudulently to withdraw millions of dollars from such individuals' and businesses' bank accounts.

(Title 18, United States Code, Sections 1030(a)(2), 1030(b), 1030(c)(2)(B)(i)-(iii), and 2.)

COUNT SEVEN

(Computer Intrusion Furthering Fraud)

The United States Attorney further charges:

32. The allegations contained in paragraphs 1 through 10 and 13 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

33. From at least in or about 2005, up to and including in or about November 2010, in the Southern District of New York and elsewhere, NIKITA KUZMIN, the defendant, knowingly and with intent to defraud, accessed and attempted to access a protected computer without authorization, and by means of such conduct furthered the intended fraud and obtained something of value exceeding $5,000, to wit, using malicious computer code known and described as the "Gozi Virus," and working with others, KUZMIN accessed and attempted to access without authorization computers owned by private individuals and businesses, and thereby obtained and attempted to obtain the bank account access information of such individuals and businesses, which information

was used fraudulently to withdraw millions of dollars from such individuals' and businesses' bank accounts.

(Title 18, United States Code,
Sections 1030(a)(4), 1030(b), 1030(c)(3)(A), and 2.)

FORFEITURE ALLEGATION AS TO COUNTS ONE AND TWO

34. As a result of committing the offense alleged in Counts One and Two of this Information, NIKITA KUZMIN, 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 offense, including but not limited to, at least approximately $50 million, a sum of money representing the amount of proceeds obtained as a result of the said offense.

FORFEITURE ALLEGATION AS TO COUNTS THREE AND FOUR

35. As a result of committing the offense alleged in Counts Three and Four of this Information, NIKITA KUZMIN, 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, including but not limited to at least approximately $50 million, a sum of money representing the amount of proceeds obtained as a result of the said offense; and

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

FORFEITURE ALLEGATION AS TO COUNTS FIVE, SIX, AND SEVEN

36. As a result of committing one or more of the offenses alleged in Counts Five, Six, and Seven of this Information, NIKITA KUZMIN, the defendant, shall forfeit to the United States, 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 offenses, including but not limited to at least approximately $50 million, a sum of money representing the amount of proceeds obtained as a result of the said offenses.

Substitute Assets Provision

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

(1) cannot be located upon the exercise of due diligence;

(2) has been transferred or sold to, or deposited with, a third person;

(3) has been placed beyond the jurisdiction of the Court;

(4) has been substantially diminished in value; or

(5) has been commingled with other property which cannot be subdivided without difficulty; it is the intent of the United States, pursuant to 21 U.S.C. § 853(p), to seek forfeiture of any other property of said defendant up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(2)(B), and 1029(c)(1)(C), Title 21, United States Code, Section 853(p), and Title 28, United States Code, Section 2461(c).)

Preet Bharara

PREET BHARARA
United States Attorney

JK