IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	Criminal No. 19-104
v.	)	
	)	**[UNDER SEAL]**
ALEXANDER KONOVOLOV	)	
a/k/a "NoNe"	)	(18 U.S.C. §§ 371, 1349 and 1956(h))
a/k/a "none_1"	)	
MARAT KAZANDJIAN	)	
a/k/a "phant0m"	)	
VLADIMIR GORIN	)	
a/k/a "Voland"	)	
a/k/a "mrv"	)	
a/k/a "riddler"	)	
GENNADY KAPKANOV	)	
a/k/a "Hennadiy Kapkanov"	)	
a/k/a "flux"	)	
a/k/a "ffhost"	)	
a/k/a "firestarter"	)	
a/k/a "User41"	)	
EDUARD MALANICI	)	
a/k/a "JekaProf"	)	
a/k/a "procryptgroup"	)	
KONSTANTIN VOLCHKOV	)	
a/k/a "elvi"	)	
RUSLAN VLADIMIROVICH KATIRKIN	)	
a/k/a "stratos"	)	
a/k/a "xen"	)	
VIKTOR VLADIMIROVICH EREMENKO	)	
a/k/a "nfcorpi"	)	
FARKHAD RAUF OGLY MANOKHIN	)	
a/k/a "frusa"	)	
ALEXANDER VAN HOOF	)	
a/k/a "al666"	)	

INDICTMENT

The grand jury charges:

Introduction

At all times material to this Indictment, unless otherwise alleged:

1. From in and around October 2015, and continuing through in and around December 2016, ALEXANDER KONOVOLOV, a/k/a "NoNe," a/k/a "none_1," MARAT KAZANDJIAN, a/k/a "phant0m," VLADIMIR GORIN, a/k/a "Voland," a/k/a "mrv," a/k/a "riddler," GENNADY KAPKANOV, a/k/a "Hennadiy Kapkanov," a/k/a "flux," a/k/a "ffhost," a/k/a "firestarter," a/k/a "User 41," KONSTANTIN VOLCHKOV, a/k/a "elvi," EDUARD MALANICI, a/k/a "JekaProf," a/k/a "procryptgroup," RUSLAN VLADIMIROVICH KATIRKIN, a/k/a "stratos," a/k/a "xen," VIKTOR VLADIMIROVICH EREMENKO, a/k/a "nfcorpi," FARKHAD RAUF OGLY MANOKHIN, a/k/a "frusa," ALEXANDER VAN HOOF, a/k/a "al666," along with conspirator Krasimir Nikolov, a/k/a "pablopicasso," a/k/a "salvadordali," a/k/a "karlo," and others, were part of a transnational organized cybercrime network that stole money from unsuspecting victims, primarily businesses and their financial institutions, through the use of GozNym malware.

2. Specifically, the defendants and others conspired to: (a) infect victims' computers with GozNym malware designed to capture victims' online banking login credentials; (b) use the captured login credentials to fraudulently gain unauthorized access to victims' online bank accounts at financial institutions; and (c) steal funds from victims' bank accounts and launder those funds using U.S. and foreign beneficiary bank accounts provided and controlled by conspirators.

3. The conspirators were located in various countries around the world including, but not limited to, Russia, Georgia, Ukraine, Moldova, Bulgaria and Kazakhstan.

4. In order to perpetrate the criminal scheme, the defendants utilized a network of co-conspirators who provided specialized technical skills and services used in furtherance of the conspiracy. The specialized skills or services included, *inter alia*, the following:

- Malware Developer: In the context of this Indictment, a "malware developer" was a conspirator involved in the creation, development, management, and leasing of malware for use by himself and/or others.

- Crypter: In the context of this Indictment, a "crypter" was a conspirator involved in encrypting malware in such a way as to avoid detection by anti-virus tools and software on victims' computers.

- Spammer: In the context of this Indictment, a "spammer" was a conspirator involved in the mass distribution of malware through phishing emails. The phishing emails were designed to appear legitimate to entice victim recipients into opening the emails and clicking on a link or attachment, which facilitated the downloading of malware onto the victims' computers.

- Bulletproof Hoster: In the context of this Indictment, a "bulletproof hoster" was a conspirator involved the hosting of malware campaigns on an intricate network of servers designed to thwart detection by law enforcement and cybersecurity researchers, thereby enabling the malware-related criminal activities to continue without disruption.

- Casher / Account Takeover Specialist: In the context of this Indictment, a "casher" or "account takeover specialist" was a conspirator who used victims' stolen login credentials (obtained through GozNym malware infections) to access the victims' online bank accounts and steal, or attempt to steal, victims' funds through electronic funds transfers.

- Cash-Out / Drop Master: In the context of this Indictment, a "cash-out" or "drop master" was a conspirator who provided "cashers / account takeover specialists" and other members of the conspiracy with access to bank accounts (also known as "drop accounts") to receive stolen funds in the form of electronic funds transfers from victims' online bank accounts. "Drop masters" utilized money mules (also known as "drops") to open drop accounts, withdraw stolen funds, or transfer stolen funds to other accounts for withdrawal.

5. The conspirators advertised, or otherwise offered, their specialized skills and services on underground, Russian-speaking, online criminal forums, including Mazafaka, Verified, and DirectConnection. The online forums provided a virtual meeting place where

vetted cybercriminals could advertise their skills and services and communicate with each other in private messages.

6. "GozNym" was the name given by computer security researchers to a particular malicious software (malware) program. GozNym was a hybrid of two previous malware strains, Gozi and Nymaim.

7. GozNym was a multifunction malware package specifically designed to automate the theft of sensitive personal and financial information, including online banking login credentials such as usernames and passwords, from infected computers.

8. GozNym infected tens of thousands of victim computers worldwide, primarily in the United States and Europe.

9. In the United States, GozNym infections primarily targeted victim computers belonging to U.S. businesses, including in the Western District of Pennsylvania.

10. After victims' online banking login credentials were captured by GozNym, the credentials were used to fraudulently gain unauthorized access to victims' online bank accounts at U.S. financial institutions, in order to transfer the victims' funds to beneficiary bank accounts controlled by members of the conspiracy.

11. Financial institutions in the United States first observed fraudulent activity related to GozNym malware in and around late 2015.

12. GozNym infections had the potential to cause in excess of $100 million in losses to businesses and their financial institutions around the world.

13. The U.S. financial institutions referenced herein that were victims of GozNym-related fraud were insured by the Federal Deposit Insurance Corporation or chartered by the United States.

14. Unless otherwise noted, all communications of conspirators set forth in this Indictment were translated from Russian to English by certified Russian linguists.

The Defendants

15. ALEXANDER KONOVOLOV, a/k/a "NoNe," a/k/a "none_1," is a national and citizen of Georgia. During the time frame of the conspiracy, KONOVOLOV resided in or near Tbilisi, Georgia, and used the online monikers "NoNe" and "none_1." KONOVOLOV was the primary organizer and leader of the GozNym conspiracy, who admitted that since 2015 he controlled more than 41,000 victim computers (known as "bots") infected with GozNym malware. KONOVOLOV's photograph is attached as **EXHIBIT A**.

16. MARAT KAZANDJIAN, a/k/a "phant0m," is a national and citizen of both Kazakhstan and Georgia. During the time frame of the conspiracy, KAZANDJIAN resided both in and around Tbilisi, Georgia, and in Kazakhstan. KAZANDJIAN, who used the online moniker "phant0m," was ALEXANDER KONOVOLOV's primary assistant and technical administrator. KAZANDJIAN's photograph is attached as **EXHIBIT B**.

17. VLADIMIR GORIN, a/k/a "Voland," a/k/a "mrv," a/k/a "riddler," is a national and citizen of Russia. During the time frame of the conspiracy, GORIN resided in Orenburg, Russia, and used the online monikers "Voland" and "mrv" and currently uses the moniker "riddler." As the "malware developer," GORIN oversaw the creation, development, management, and leasing of GozNym malware to conspirators, including to ALEXANDER KONOVOLOV. GORIN's photograph is attached as **EXHIBIT C**.

18. GENNADY KAPKANOV, a/k/a "Hennadiy Kapkanov," a/k/a "flux," a/k/a "ffhost," a/k/a "firestarter," a/k/a "User41," is a national and citizen of Ukraine. During the time frame of the conspiracy, KAPKANOV resided in Poltava, Ukraine, and used the online monikers "flux," "ffhost," "firestarter," and "User41." KAPKANOV was an administrator of a bulletproof

hosting services network, named by computer security researchers as the "Avalanche" network, which provided services to more than 200 cybercriminals, including defendants ALEXANDER KONOVOLOV and MARAT KAZANDJIAN. GENNADY KAPKANOV provided hosting services to more than twenty different malware campaigns, including GozNym. KAPKANOV's photograph is attached as **EXHIBIT D**.

19. EDUARD MALANICI, a/k/a "JekaProf," a/k/a "procryptgroup," is a national and citizen of Moldova. During the time frame of the conspiracy, MALANICI resided in Balti, Moldova, and used the online monikers "JekaProf" and "procryptgroup." MALANICI, a provider of crypting services, crypted GozNym malware on behalf of the charged conspiracy to enable the malware to avoid detection by anti-virus tools and software on victims' computers. MALANICI's photograph is attached as **EXHIBIT E**.

20. KONSTANTIN VOLCHKOV, a/k/a "elvi," is a national and citizen of Russia. During the time frame of the conspiracy, VOLCHKOV resided in Moscow, Russia, and used the online moniker "elvi." VOLCHKOV, a provider of spamming services, conducted spamming operations of GozNym malware on behalf of the charged conspiracy. The spamming operations involved the mass distribution of GozNym malware through phishing emails. The phishing emails were designed to appear legitimate to entice victim recipients into opening the emails and clicking on a link or attachment, which facilitated the downloading of GozNym onto the victims' computers. A photograph of VOLCHKOV was not available.

21. RUSLAN VLADIMIROVICH KATIRKIN, a/k/a "stratos," a/k/a "xen," is a national and citizen of Kazan, Russia. During the time frame of the conspiracy, KATIRKIN resided in Khmelnytskyi, Ukraine, and used the online monikers "stratos" and "xen." KATIRKIN, a "casher" or "account takeover specialist" on behalf of the charged conspiracy, used victims' stolen banking login credentials captured by GozNym infections to fraudulently

gain unauthorized access to victims' online bank accounts and steal, or attempt to steal, victims' funds through electronic funds transfers. KATIRKIN's photograph is attached as **EXHIBIT F**.

22. VIKTOR VLADIMIROVICH EREMENKO, a/k/a, "nfcorpi," is a national and citizen of Russia. During the time frame of the conspiracy, EREMENKO resided in Stavropol, Russia and used the online moniker "nfcorpi." EREMENKO, a "cash-out" or "drop master" on behalf of the charged conspiracy, provided ALEXANDER KONOVOLOV and his "cashers" / "account takeover specialists" with access to bank accounts (also known as "drop accounts") controlled by EREMENKO to receive stolen funds from victims' online bank accounts. EREMENKO's photograph is attached as **EXHIBIT G**.

23. FARKHAD RAUF OGLY MANOKHIN, a/k/a "frusa," is a national and citizen of Russia. During the time frame of the conspiracy, MANOKHIN resided in Volograd, Russia, and used the online moniker "frusa." MANOKHIN, a "cash-out" or "drop master" on behalf of the charged conspiracy, provided ALEXANDER KONOVOLOV and his "cashers" / "account takeover specialists" with access to bank accounts (also known as "drop accounts") controlled by MANOKHIN to receive stolen funds from victims' online bank accounts. MANOKHIN traveled from Russia to Sri Lanka in February 2017. At the request of the United States, MANOKHIN was arrested by Sri Lankan authorities on federal criminal charges filed against him in the United States. Following his arrest, MANOKHIN was released on bail but was required to remain in Sri Lanka pending the outcome of the extradition request of the United States. In December 2017, MANOKHIN unlawfully absconded from Sri Lanka to Russia prior to the conclusion of the extradition proceedings. MANOKHIN's photograph is attached as **EXHIBIT H**.

24. ALEXANDER VAN HOOF, a/k/a "al666," is a national and citizen of Ukraine. During the time frame of the conspiracy, VAN HOOF resided in Nikolaev, Ukraine, and used the

online moniker "al666." VAN HOOF, a "cash-out" or "drop master" on behalf of the charged conspiracy, provided ALEXANDER KONOVOLOV and his "cashers" / "account takeover specialists" with access to bank accounts (also known as "drop accounts") controlled by VAN HOOF to receive stolen funds from victims' online bank accounts. VAN HOOF's photograph is attached as **EXHIBIT I**.

Conspirator Charged in Related Indictment

25. Conspirator Krasimir Nikolov, a/k/a "pablopicasso," a/k/a "salvadordali," a/k/a "karlo," a national and citizen of Bulgaria, is the subject of a related Indictment at Criminal No. 16-218 (WDPa.) During the time frame of the conspiracy, Nikolov resided in Varna, Bulgaria, and used the online monikers "pablopicasso," "salvadordali" and "karlo." Nikolov, a "casher" or "account takeover specialist" on behalf of the charged conspiracy, used victims' stolen banking credentials captured by GozNym malware infections to access the victims' online bank accounts and steal, or attempt to steal, victims' funds through electronic funds transfers. At the request of the United States, Nikolov was arrested in Bulgaria and extradited to the Western District of Pennsylvania in December 2016.

COUNT ONE
(Conspiracy to Commit Computer Fraud)

The grand jury charges:

Statutory Allegations

26. From in and around October 2015, and continuing thereafter to in and around December 2016, in the Western District of Pennsylvania and elsewhere, ALEXANDER KONOVOLOV, a/k/a "NoNe," a/k/a "none_1," MARAT KAZANDJIAN, a/k/a "phant0m," VLADIMIR GORIN, a/k/a "Voland," a/k/a "mrv," a/k/a "riddler," GENNADY KAPKANOV, a/k/a "Hennadiy Kapkanov," a/k/a "flux," a/k/a "ffhost," a/k/a "firestarter," a/k/a "User 41," KONSTANTIN VOLCHKOV, a/k/a "elvi," EDUARD MALANICI, a/k/a "JekaProf," a/k/a "procryptgroup," RUSLAN VLADIMIROVICH KATIRKIN, a/k/a "stratos," a/k/a "xen." VIKTOR VLADIMIROVICH EREMENKO, a/k/a "nfcorpi," FARKHAD RAUF OGLY MANOKHIN, a/k/a "frusa," ALEXANDER VAN HOOF, a/k/a "al666," and conspirator Krasimir Nikolov, a/k/a "pablopicasso," a/k/a "salvadordali," a/k/a "karlo," knowingly and intentionally conspired and agreed with each other, and with persons known and unknown to the grand jury, (collectively, the conspirators) to commit offenses against the United States, that is:

a. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage, and attempt to cause damage, without authorization, to a protected computer, and cause loss to one or more persons during a 1-year period aggregating at least $5,000.00 in value and damage affecting 10 or more protected computers during a 1-year period, in violation of Title18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B)(i);

b. to knowingly and with intent to defraud, access a protected computer without authorization, and by means of such conduct further the intended fraud and obtain anything of value exceeding $5,000 in any 1-year period, in violation of Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A).

Objectives of the Conspiracy

27. The objectives of the conspiracy included: (a) infecting victims' computers with GozNym malware designed to capture victims' online banking login credentials; (b) using the captured login credentials to gain unauthorized access to victims' online bank accounts at U.S. financial institutions; and (c) stealing funds from victims' U.S. bank accounts and laundering those funds using U.S. and foreign beneficiary bank accounts provided and controlled by conspirators.

Manner and Means of the Conspiracy

28. The manner and means used to accomplish the conspiracy's objectives included the following:

29. Each conspirator provided a specialized technical skill or service used in furtherance of the conspiracy. The conspirators advertised, or otherwise offered, their specialized skills and services on underground, Russian-speaking, online criminal forums.

30. VLADIMIR GORIN, a/k/a "Voland," a/k/a "mrv," a/k/a "riddler," oversaw the creation, development, management, and leasing of GozNym malware. GORIN provided GozNym to ALEXANDER KONOVOLOV, a/k/a "NoNe," a/k/a "none_1."

31. ALEXANDER KONOVOLOV, the leader and primary organizer of the conspiracy, formed much of the conspiracy by meeting and recruiting conspirators through underground, Russian-speaking, online criminal forums.

32. GENNADY KAPKANOV, a/k/a "Hennadiy Kapkanov," a/k/a "flux," a/k/a "ffhost," a/k/a "firestarter," a/k/a "User41," was an administrator of the Avalanche bulletproof hosting service. The service provided co-conspirators and other cybercriminals with a secure platform to conduct malware and money mule campaigns without the fear of detection or disruption by law enforcement or cybersecurity researchers.

33. GENNADY KAPKANOV provided bulletproof hosting services to ALEXANDER KONOVOLOV and MARAT KAZANDJIAN in furtherance of the GozNym conspiracy.

34. GENNADY KAPKANOV offered co-conspirators and other cybercriminals various services, in exchange for a fee, including the following: (a) the registering of malware and money mule-related domains with numerous domain registrars in several countries, including Malaysia, Pakistan, Russia, India, and China; (b) the hosting of malware on Avalanche servers that infected victim computers; and (c) the "proxying" (passing) of information and data from victims' computers through a layered, or tiered, network of servers and finally to back-end servers where it was ultimately accessed by Avalanche's malware customers.

35. GENNADY KAPKANOV advertised the bulletproof hosting services to cybercriminals on underground, Russian-speaking, online criminal forums, including Verified and Mazafaka. An advertisement for KAPKANOV's services on the Verified and Mazafaka forums are attached as **EXHIBITS J** and **K**, respectively.

36. GENNADY KAPKANOV described a portion of his services during the following communication on or about April 8, 2016, with a potential customer who inquired about Avalanche's hosting services:

- CUSTOMER: Servers are needed for lease...
- KAPKANOV: ...for what purposes are the servers needed?
- CUSTOMER: Botnet controller. An abuse complaint comes to one server, on average, once a month.
- KAPKANOV: We can suggest fast-fluxing. You can buy them at any clean data center or you can buy a VPS. With the required configuration of the hardware, we proxy the traffic from your bots to your server, thus it becomes bulletproof since all of the abuse of service complaints come to us. The price is 150 Web money per week or 450 Web money for 4 weeks.

37. GENNADY KAPKANOV and his fellow administrator leased access to servers from legitimate hosting providers using fictitious names or the names of unwitting third parties. The servers were often leased using stolen credit cards.

38. VLADIMIR GORIN, ALEXANDER KONOVOLOV, and MARAT KAZANDJIAN collaborated with GENNADY KAPKANOV in the registering of malicious GozNym domains, the hosting of GozNym executable files on KAPKANOV's servers for infecting victim computers, and the proxying of information from infected GozNym computers through the Avalanche network where it was accessible at a back-end server.

39. The conspirators crypted GozNym malware to enable the malware to avoid detection by anti-virus tools and software on victims' computers. EDUARD MALANICI, a/k/a "JekaProf," a/k/a "procryptgroup," and others known and unknown to the grand jury, crypted GozNym malware on behalf the conspiracy.

40. The conspirators distributed GozNym malware and infected victim computers through spamming. KONSTANTIN VOLCHKOV, a/k/a "elvi," and others known and unknown to the grand jury, conducted spamming of GozNym malware on behalf of the conspiracy.

41. The spamming involved sending malicious phishing emails through the internet to large numbers of victims, primarily U.S. businesses. The emails falsely represented themselves to be legitimate emails from companies, associations, and organizations.

42. The conspirators designed the phishing emails to fraudulently entice victim recipients to click on a hyperlink or attachment that falsely represented itself to be a legitimate link or attachment, such as business invoice. When the victim clicked on the link or attachment, the victim's computer was typically redirected to a malicious domain controlled by conspiracy, from which GozNym malware was downloaded onto the victim's computer without the victim's knowledge or consent.

43. The conspirators used GozNym malware on infected victim computers to capture the victims' confidential personal and financial information, including online banking login credentials, by keystroke logging and/or web injects (i.e., fake online banking webpages).

44. Keystroke logging recorded (or logged) the keys struck on a victim's keyboard. The keystrokes were captured surreptitiously by the computer program (i.e., keylogger) without the victim's knowledge. Through keystroke logging, conspirators stole victims' online banking credentials when the victims logged into their online bank account from their infected computer.

45. Web injects introduced (or injected) malicious computer code into a victim's web browser while the victim browsed the Internet and "hijacked" the victim's Internet session. Web injects were used to display false online banking pages into the victim's web browser to trick the victim into entering online banking information, which was then captured by the conspirators.

46. To defeat two-factor authentication and RSA tokens needed to access many online bank accounts, the conspirators created and utilized a GozNym token panel in furtherance of the conspiracy. A screen shot of the GozNym token panel is attached as **EXHIBIT L**.

47. The token panel was an interface hosted on a server that was configured to allow conspirators to see the victims that had been infected with GozNym malware along with the victims' confidential banking information captured by GozNym malware. The confidential information displayed on the token panel included usernames, passwords and answers to security questions needed for accessing victims' online bank accounts. Using web injects designed to look like the legitimate online banking webpage of a victims' financial institutions, the token panel enabled the conspirators to interact with the employees of victim businesses and enticed the employees to enter their RSA token code into the fake online banking webpages.

48. The conspirators, including VLADIMIR GORIN, ALEXANDER KONOVOLOV, MARAT KAZANDJIAN, RUSLAN VLADIMIROVICH KATIRKIN, and

Krasimir Nikolov, all used a VNC (Virtual Network Computing) connection hosted at IP address 162.244.32.157 to remotely control victims' computers in furtherance of the conspiracy.

49. The conspirators used the victims' stolen banking credentials without authorization to falsely represent to banks that conspirators were victims (or employees of victims) who had authorization to access the victims' bank accounts and to make electronic funds transfers from the victims' bank accounts.

50. The conspirators used the stolen banking credentials to gain unauthorized access to victims' online bank accounts and caused, and attempted to cause, banks to make unauthorized wire transfers, ACH payments, or other electronic funds transfers from the victims' bank accounts, without the knowledge or consent of the victim account holders.

51. Defendant RUSLAN VLADIMIROVICH KATIRKIN and conspirator Krasimir Nikolov (charged in the related Indictment at Criminal No. 16-218) , were two "cashers" or "account takeover specialists" who utilized the token panel to access victims' online bank accounts to steal, or attempt to steal, victims' funds through electronic funds transfers.

52. The earliest identified token panel used the domain fokentoken.com and was hosted at IP address 204.155.30.87. Subsequent panels were hosted at IP address 204.155.31.133, and thereafter at IP address 204.155.30.8.

53. The conspirators used U.S. and foreign bank accounts (also known as "drop accounts") provided and controlled by other members of the conspiracy to receive stolen funds, in the form of electronic funds transfers, from victims' online bank accounts. The conspirators who controlled the drop accounts were known as "cash-outs" or "drop masters" and included, among others, VLADIMIROVICH EREMENKO, a/k/a, "nfcorpi," FARKHAD RAUF OGLY MANOKHIN, a/k/a "frusa," and ALEXANDER VAN HOOF, a/k/a "al666."

54. The "cash-outs" or "drop masters" sometimes employed "drops," also known as "money mules," who were directed to move the stolen funds to other accounts and "cash out" the stolen funds from the "drop accounts."

55. The conspirators divided the stolen funds accordingly based upon previously-negotiated percentage sharing agreements.

Overt Acts

56. In furtherance of the conspiracy, and to achieve the goals and objectives of the conspiracy, the defendants, and other conspirators known and unknown to the grand jury, did commit and cause to be committed, the following overt acts, *inter alia*, in the Western District of Pennsylvania and elsewhere:

a. Administrative and Technical Tasks Conducted in Furtherance of the Conspiracy

57. On or about October 5, 2015, VLADIMIR GORIN conducted on online search for "phant0m on token server," a reference to MARAT KAZANDJIAN, a/k/a "phant0m," and his involvement with the GozNym token server.

58. On or about October 24, 2015, ALEXANDER KONOVOLOV and Krasimir Nikolov communicated regarding the criminal scheme that included details of how the botnet would operate, the financial institutions that would be targeted, and other conspirators, such as "phant0m" (i.e., MARAT KAZANDJIAN) who would be involved in the scheme.

59. On or about November 5, 2015, ALEXANDER KONOVOLOV communicated with Krasimir Nikolov regarding bank accounts ("drop accounts") available to receive stolen funds. KONOVOLOV sent Nikolov the details for a bank account at Ally Bank provided and controlled by defendant ALEXANDER VAN HOOF, a/k/a "al666."

60. On or about November 10, 2015, VLADIMIR GORIN posted on an underground online criminal forum that those who wished to rent a malware "Trojan" (i.e., GozNym) from him have: (a) quality loads; (b) viable cash-out schemes; and (c) launderers / exchangers.

61. On or about November 22, 2015, MARAT KAZANDJIAN sent Krasimir Nikolov a message containing the domain hXXp://fokentoken.com/concert5/index.php?r=admin/index, along with the password "qwerty123," which provided Nikolov with access to the GozNym token panel hosted on a server at IP address 204.155.30.87.

62. On or about December 7, 2015, MARAT KAZANDJIAN sent Krasimir Nikolov a message that explained how to login to the GozNym token panel.

63. On or about January 15, 2016, MARAT KAZANDJIAN sent Krasimir Nikolov a message containing the IP address 204.155.31.133 which hosted the GozNym token panel after it was moved from the previous server at IP address 204.155.30.87.

64. On or about January 18, 2016, ALEXANDER KONOVOLOV discussed with VLADIMIR GORIN a potential delay in GozNym-related activities. GORIN stated that he "won't be keeping the bots loaded on the old server very long." KONOVOLOV asked GORIN if he will still be able to start spamming at "12 midnight, Moscow time, on the 20th." GORIN replied, "the probability of starting on the 20th is 80%." KONOVOLOV complained, "So sh*t this is such a mess....now I have 4 people to switch." Shortly thereafter, KONOVOLOV sent a copy of his communications with GORIN to both GENNADY KAPKANOV and Krasimir Nikolov and advised, "We have a problem."

65. On or about January 18, 2016, GENNADY KAPKANOV sent ALEXANDER KONOVOLOV and MARAT KAZANDJIAN a message containing the login name and password to access Avalanche's domain registration ("dreg") panel. The dreg panel allowed

users to register new malicious domains and check on the status of previously-registered domains.

66. During the time frame of the conspiracy, GENNADY KAPKANOV maintained a "buddy list" containing the online monikers of his criminal associates. KAPKANOV assigned each criminal associate a corresponding numerical designation. User "250" was the numerical designation for "none_1" (i.e., ALEXANDER KONOVOLOV) and User "250 admin" was the numerical designation for "phant0m" (i.e., MARAT KAZANDJIAN). A screen shot of KAPKANOV's numerical designations for "none_1" and "phant0m" is attached as **EXHIBIT M**.

67. On or about January 25, 2016, MARAT KAZANDJIAN sent Krasimir Nikolov a message containing information for a fraudulent invoice. This invoice was consistent with those used in the GozNym phishing emails that were designed to appear legitimate to entice the recipient to click on it.

68. On or about February 29, 2016, defendant KONSTANTIN VOLCHKOV, a/k/a "elvi," received a message from a conspirator stating, "Hi. I'm from None in regard to spam." VOLCHKOV and the conspirator then discussed the details of VOLCHKOV's GozNym spamming efforts, including that the spam emails were to be directed to employees at large and small businesses, and each email was to be crafted to include the address of the business and the name of the employee targeted. VOLCHKOV explained, "There will be the database, the 'from,' the name of the 'from,' the subject, and the message, and a place in the message where to put the name."

69. On or about March 1, 2016, the conspirator sent KONSTANTIN VOLCHKOV the links to two sendspace.com files, and stated, "The password is None." The conspirator then

asked VOLCHKOV, "At what time will the spam be available?" VOLCHKOV replied, "I have no f***ing idea yet. They are preparing the documents."

70. On or about March 4, 2016, ALEXANDER KONOVOLOV sent a conspirator a copy of the communications KONOVOLOV had with defendant EDUARD MALANICI, a/k/a "JekaProf," a/k/a "procryptgroup," regarding the crypting of GozNym malware in furtherance of the conspiracy. MALANICI stated, "I'll make a loader for you so that the ping is normal." KONOVOLOV replied, "ok. It's needed tomorrow for my spammer." KONOVOLOV asked, "Will the bots survive long?" MALANICI replied, "Encrypt them and they won't die." KONOVOLOV replied, "I'll contact you as soon as the spammer shows up tomorrow."

71. During the time frame of the conspiracy, GENNADY KAPKANOV and his fellow Avalanche administrator registered dozens of malicious GozNym domains on behalf of ALEXANDER KONOVOLOV and MARAT KAZANDJIAN, and maintained a list of those malicious domains on a domain registration table.

72. On or about March 7, 2016, GENNADY KAPKANOV and ALEXANDER KONOVOLOV discussed and passed in messages numerous malicious GozNym domains, including "secureserver17.com."

73. On or about March 15, 2016, GENNADY KAPKANOV and MARAT KAZANDJIAN discussed and passed in messages a malicious GozNym domain identified as "hXXp://secureserver17.com/home/res509.exe" that KAPKANOV then hosted on Avalanche servers where it was used to infect victims' computers.

74. On or about March 16, 2016, GENNADY KAPKANOV and MARAT KAZANDJIAN discussed and passed in messages a malicious GozNym domain identified as "secureserver18.com" that KAPKANOV then hosted on Avalanche servers where it was used to infect victims' computers.

75. On or about March 25, 2016, ALEXANDER KONOVOLOV directed a conspirator to contact EDUARD MALANICI, a/k/a "JekaProf," a/k/a "procryptgroup," regarding additional GozNym crypting. KONOVOLOV stated, "Contact procryptgroup@exploit.im." The conspirator replied, "I already contacted him." KONOVOLOV advised, "He'll load for you with certainty that it won't be an excessive load and die. You'll see how the bot pings and how it works." The conspirator replied, "He has already loaded everything."

76. On or about April 11, 2016, defendant RUSLAN VLADIMIROVICH KATIRKIN, a/k/a "stratos," a/k/a "xen," accessed the GozNym token panel hosted at IP address 204.155.31.133; the same IP address MARAT KAZANDJIAN sent to Krasimir Nikolov on January 15, 2016.

77. On or about April 15, 2016, RUSLAN VLADIMIROVICH KATIRKIN confirmed with a conspirator that he (KATIRKIN) was "on None's token," a reference to KATIRKIN's "casher" / "account takeover specialist" activities using the GozNym token panel.

78. On or about April 27, 2016, MARAT KAZANDJIAN sent conspirator Krasimir Nikolov the link to access the GozNym token panel after it was moved to a new hosting server at IP address 204.155.30.8.

79. On May 26, 2016, KONSTANTIN VOLCHKOV sent a message to GENNADY KAPKANOV and stated, "None told me to call you, in regard to domains."

b. Attacks on Specific Victims

80. GozNym infected tens of thousands of victim computers worldwide, including in the Western District of Pennsylvania, and had the potential to cause in excess of $100 million in losses to businesses and their financial institutions, including the following:

(1) Victim 1

81. Victim 1 was an asphalt and paving business located in New Castle, Pennsylvania, in the Western District of Pennsylvania.

82. On or about February 16, 2016, ALEXANDER KONOVOLOV sent GENNADY KAPKANOV a message containing a malicious GozNym domain identified as "hXXp://www/billpay-center/com."

83. GENNADY KAPKANOV thereafter hosted the malicious domain on Avalanche servers where it was used to infect victims' computers with GozNym, including Victim 1's computers. KAPKANOV maintained the "billpay-center.com" domain on the domain registration user table, as seen in a screen shot attached as **EXHIBIT N**.

84. On or about February 18, 2016, the conspirators sent Victim 1's employee a phishing email designed to look like a legitimate email from Bank of America. A copy of the phishing email is attached as **EXHIBIT O**. The email contained a link identified as "invoice_0028556.doc." The source code of the phishing email showed that when the recipient clicked on the link "invoice_0028556.doc," the recipient was directed to the website hXXp://www.billpay-center.com/invoices/invoice_0028556 where a GozNym executable file was downloaded and the recipient's computer was infected with GozNym malware.

85. On or about February 18, 2016, the conspirators fraudulently enticed Victim 1's employee to click on the link "invoice_0028556.doc" and, in doing so, caused the installation of GozNym malware on Victim 1's computer.

86. On or about February 22, 2016, ALEXANDER KONOVOLOV sent Krasimir Nikolov the details for a Bank of America account in the name DC Services by Hinkley, along with a notation that the account was authorized to receive between $50,000.00 to $100,000.00 in

funds. Additionally, KONOVOLOV sent Nikolov a username and password that to electronically access the account.

87. On or about February 24, 2016, the conspirators used GozNym malware to fraudulently obtain Victim 1's online banking credentials and attempted to cause three unauthorized electronic funds transfers totaling $121,132.08 from Victim 1's bank account at First National Bank, located in the Western District of Pennsylvania, to beneficiary bank accounts controlled by conspirators. Two electronic funds transfers totaling $114,144.68 were destined for the same Bank of America account in the name DC Services by Hinkley that ALEXANDER KONOVOLOV provided to Krasimir Nikolov on or about February 22, 2016.

88. On or about April 11, 2016, Krasimir Nikolov sent a conspirator a message containing Victim 1's business name, as well as Victim 1's business email account.

89. On or about April 11, 2016, Krasimir Nikolov received from conspirators detailed information regarding four beneficiary bank accounts designated to receive funds stolen from GozNym victims, including Victim 1.

90. On or about April 12, 2016, Nikolov gained unauthorized access to Victim 1's First National Bank account using Victim 1's online banking credentials captured by GozNym malware, and attempted to cause four electronic funds transfers totaling $122,000.00, from Victim 1's account to the same four beneficiary bank accounts provided to Nikolov by conspirators on or about April 11, 2016.

(2) Victim 2

91. Victim 2 was a law firm located in Washington, DC.

92. On or about February 16, 2016, ALEXANDER KONOVOLOV sent GENNADY KAPKANOV a message containing a malicious GozNym domain identified as

"hXXp://www/billpay-center/com/invoice#007448322." A screen shot of the message is attached as **EXHIBIT P**.

93. GENNADY KAPKANOV then hosted the malicious domain on Avalanche servers where it was used to infect victims' computers with GozNym malware, including Victim 2's computers.

94. On or about February 16, 2016, the conspirators sent a phishing email to Victim 2's employee designed to look like a legitimate email from "Quicken Billpay-center." A copy of the phishing email is attached as **EXHIBIT Q**. The email directed the recipient to "Click the link below to view your Invoice." The link was identified as "hXXp://www/billpay-center/com/invoice#007448322," and was the same malicious link passed from ALEXANDER KONOVOLOV to GENNADY KAPKANOV earlier that same date. Clicking on the link caused a GozNym malware executable file to be downloaded and the recipient's computer to be infected with GozNym malware.

95. On or about February 16, 2016, the conspirators fraudulently enticed Victim 2's employee to click on the link "hXXp://www/billpay-center/com/invoice#007448322" and, in doing so, caused the installation of GozNym malware on Victim 2's computer.

96. On or about February 25, 2016, ALEXANDER KONOVOLOV and Krasimir Nikolov passed messages containing the details for a beneficiary bank account ending in 8231 in the name Cane Inc., P.O. Box 3, Whitinsville, MA.

97. On or about February 25, 2016, Krasimir Nikolov gained unauthorized access to Victim 2's Bank of America account using Victim 2's online banking credentials captured by GozNym malware, and attempted to cause an unauthorized electronic funds transfer totaling $97,520.00 from Victim 2's account to the same beneficiary bank account ending in 8231 in the

name Cane, Inc. passed earlier that date between ALEXANDER KONOVOLOV and Krasimir Nikolov. This transaction resulted in a loss of $76,178.12.

(3) Victim 3

98. Victim 3 was a church was located in Southlake, Texas.

99. On or about February 11, 2016, conspirators gained unauthorized access to Victim 3's Wells Fargo Bank account using Victim 3's online banking credentials captured by GozNym malware, and attempted to cause three unauthorized electronic funds transfer totaling $610,440.00 from Victim 3's bank account to beneficiary bank accounts provided and controlled by the conspirators. Specifically, one electronic funds transfer totaling $217,440.00 was destined for a bank account ending in 5091 in the name Orto LP at Norvik Banka, JSC in Riga, Latvia, provided and controlled by defendant VIKTOR VLADIMIROVICH EREMENKO, a/k/a "nfcorpi."

100. On or about February 21, 2016, ALEXANDER KONOVOLOV and Krasimir Nikolov discussed and passed the malicious GozNym domain "hXXp://intuit.secureserver17.com/invoices/invoice_897-84-579.doc."

101. On or about February 22, 2016, in an effort to re-infect Victim 3's computers with GozNym, the conspirators sent Victim 3's employee a subsequent phishing email designed to look like a legitimate email from Bank of America. The email, attached as **EXHIBIT R**, looked nearly identical to the phishing email sent by the conspirators to Victim 1. The phishing email contained a link identified as "invoice_897-84579.doc." The source code of the phishing email showed that when the recipient clicked on the link "invoice_897-84579.doc," the recipient's computer was directed to the website "hXXp://intuit.secureserver17.com/invoices/invoice_897-84-579.doc" (i.e., the same domain discussed and passed between ALEXANDER KONOVOLOV and Krasimir Nikolov on February 21, 2016). At this website, a GozNym

executable file was downloaded and the recipient's computer was infected with GozNym malware.

102. On or about February 22, 2016, the conspirators fraudulently enticed Victim 3's employee to click on the link hXXp://intuit.secureserver17.com/invoices/invoice_897-84-579.doc and, in doing so, caused a subsequent installation of GozNym malware on Victim 3's computer.

103. The domain "secureserver17.com" was the same malicious GozNym domain discussed and passed by GENNADY KAPKANOV and ALEXANDER KONOVOLOV on March 7, 2016, and by GENNADY KAPKANOV and MARAT KAZANDJIAN on March 15, 2016.

104. The malicious GozNym domain "secureserver17.com" was hosted by GENNADY KAPKANOV on Avalanche servers and was used to infect victim computers with GozNym malware, including at Victim 3.

(4) Victim 4

105. Victim 4 was an association dedicated to providing recreation programs and other services to persons with disabilities located in Downers Grove, Illinois.

106. On or about March 16, 2016, GENNADY KAPKANOV and MARAT KAZANDJIAN discussed and passed in messages the malicious GozNym domain "secureserver18.com."

107. The malicious GozNym domain "secureserver18.com" was hosted by GENNADY KAPKANOV on Avalanche servers and was used to infect victims' computers with GozNym malware, including Victim 4's computers.

108. On or about March 16, 2016, the conspirators sent Victim 4's employee a phishing email designed to look like a legitimate business email. The email contained a link to

the malicious GozNym domain "secureserver18.com." Clicking on the link caused a GozNym malware executable file to be downloaded and the recipient's computer to be infected with GozNym malware.

109. On or about March 16, 2016, the conspirators fraudulently enticed Victim 4's employee to click on a link in a phishing email and, in doing so, caused the installation of GozNym malware on Victim 4's computer.

110. On or about March 25, 2016, ALEXANDER KONOVOLOV sent Krasimir Nikolov a message containing the account details for several beneficiary bank accounts in Tbilisi, Georgia.

111. On or about March 25, 2016, Krasimir Nikolov gained unauthorized access to Victim 4's BankFinancial account using Victim 4's online banking credentials captured by GozNym malware, and attempted to cause two unauthorized electronic funds transfer totaling $108,300.00 from Victim 4's account to beneficiary bank accounts provided and controlled by conspirators. The beneficiary accounts designated to receive Victim 4's stolen funds included the specific bank account in Tbilisi, Georgia, sent by ALEXANDER KONOVOLOV to Krasimir Nikolov earlier that same date.

(5) Victim 5

112. Victim 5 was a distributor of neurosurgical and medical equipment headquartered in Freiburg, Germany, with a U.S. subsidiary in Cape Coral, Florida.

113. On or about March 7, 2016, defendant FARKHAD RAUF OGLY MANOKHIN, a/k/a "frusa," provided conspirators with access to a bank account at Santander Bank, N.A., in the name of B.H., K Inc. for the purpose of receiving stolen funds from Victim 5's Bank of America account.

114. On or about March 7, 2016, conspirators gained unauthorized access to Victim 5's Bank of America account using Victim 5's online banking credentials captured by GozNym malware, and caused and attempted to cause an electronic funds transfer of $98,900.00 from Victim 5's account to the Santander Bank account in the name of B.H., K Inc. provided and controlled by FARKHAD RAUF OGLY MANOKHIN. This transaction resulted in a loss of $98,900.00.

115. On or about March 8, 2016, FARKHAD RAUF OGLY MANOKHIN sent ALEXANDER KONOVOLOV a screen shot of a confirmation of the electronic funds transfer of $98,900.00 from Victim 5's bank account to the Santander Bank beneficiary account provided and controlled by MANOKHIN.

116. On or about March 8, 2016, FARKHAD RAUF OGLY MANOKHIN advised ALEXANDER KONOVOLOV of his concern that his "drop had run off" and had stolen the $98,900.00 from the conspirators. After MANOKHIN advised that he would re-send the wire transfer, KONOVOLOV stated, "Send it to…nfcorpi" (a/k/a VIKTOR VLADIMIROVICH EREMENKO).

117. On or about March 16, 2016, FARKHAD RAUF OGLY MANOKHIN contacted VIKTOR VLADIMIROVICH EREMENKO, a/k/a "nfcorpi." The communication from MANOKHIN began, "Hi. I'm from NoNe." EREMENKO replied, "Understood." MANOKHIN and EREMENKO collaborated on the receipt and transfer of stolen funds using their respective bank accounts (drop accounts).

(6) Victim 6

118. Victim 6 was a furniture business located in Chula Vista, California.

119. On or about March 25, 2016, Nikolov sent a co-conspirator a message containing the email address of an employee at Victim 6, along with an account passcode "XXXXX1959!."

120. On or about March 25, 2016, Nikolov sent a KONOVOLOV a message containing the following information: "$70,000.00 03/25/2016 [Victim 6's name]," along with the specific name and account number of the beneficiary account at VTB Bank in Tbilisi, Georgia.

121. On or about March 25, 2016, Nikolov gained unauthorized access to Victim 6's CommerceWest bank account using online banking credentials captured by GozNym malware, and attempted to cause ten electronic funds transfers totaling $737,550.00, from Victim 6's bank account to beneficiary accounts at VTB Bank in Tbilisi, Georgia, provided and controlled by the conspirators.

(7) Victim 7

122. Victim 7 was a provider of electrical safety devices located in Cumberland, Rhode Island.

123. On or about March 25, 2016, ALEXANDER KONOVOLOV directed Krasimir Nikolov to send him the name and account details for a bank account at a bank located in Tbilisi, Georgia, that was provided and controlled by conspirators.

124. On or about March 30, 2016, conspirators gained unauthorized access to Victim 7's Bank of America account using online banking login credentials captured by GozNym malware, and attempted to cause, and did cause, an electronic funds transfer in the amount of $199,777.00 from Victim 7's Bank of America account to a beneficiary account in the same name and at the same bank in Tbilisi, Georgia, that Nikolov provided to KONOVOLOV on or about March 25, 2016. The fraudulent transaction resulted in a loss of $199,777.00.

125. On or about March 31, 2016, conspirators again gained unauthorized access to Victim 7's Bank of America account using online banking login credentials captured by GozNym malware, and attempted to cause an electronic funds transfer in the amount of

$195,000.00 from Victim 7's Bank of America account to a beneficiary account at a bank in Tbilisi, Georgia, provided and controlled by a conspirator.

(8) Victim 8

126. Victim 8 was a contracting business located in Warren, Michigan.

127. On or about April 5, 2016, conspirators sent Victim 8's employee a phishing email and attachment designed to look legitimate, which enticed the employee to click on the attachment and, in doing so, caused the installation of GozNym malware on Victim 8's computer.

128. On or about April 11, 2016, FARKHAD RAUF OGLY MANOKHIN provided conspirators with access to a bank account ending in 3663 in the name of JST at Bank of America, for the purpose of receiving stolen funds via an electronic funds transfer from Victim 8's Comerica Bank account.

129. On or about April 11, 2016, RUSLAN VLADIMIROVICH KATIRKIN gained unauthorized access to Victim 8's Comerica bank account using Victim 8's online banking credentials captured by GozNym malware, and attempted to cause two unauthorized electronic funds transfers totaling $128,000.00 to bank accounts provided and controlled by conspirators. One electronic funds transfer totaling $79,000.00 was destined for the Bank of America account ending in 3663 in the name of JST provided and controlled by FARKHAD MANOKHIN. The transaction resulted in a loss of $28,000.00.

(9) Victim 9

130. Victim 9 was a provider of cold pack shipping products located in Moon, Pennsylvania, in the Western District of Pennsylvania.

131. On or about April 5, 2016, defendant FARKHAD RAUF OGLY MANOKHIN provided conspirators with access to a Citibank, N.A. bank account ending in 6728 in the name

of I.Z., for the purpose of receiving stolen funds via an electronic funds transfer from Victim 9's account at First National Bank of Pennsylvania.

132. On or about April 8, 2016, conspirators gained unauthorized access to Victim 9's account at First National Bank of Pennsylvania using Victim 9's online banking credentials captured by GozNym malware, and attempted to cause an electronic funds transfer of $19,000.00 from Victim 9's account to the Citibank, N.A. account ending in 6728 in the name of I.Z., provided and controlled by FARKHAD RAUF OGLY MANOKHIN.

(10) Victim 10

133. Victim 10 was a bolt manufacturing company located in Carnegie, Pennsylvania, in the Western District of Pennsylvania.

134. On or about April 7, 2016, conspirators sent Victim 10's employee a phishing email and attachment designed to look legitimate, which enticed the employee to click on the attachment and, in doing so, caused the installation of GozNym malware on Victim 10's computer.

135. On or about April 11, 2016, defendant RUSLAN VLADIMIROVICH KATIRKIN gained unauthorized access to Victim 10's PNC Bank account from the GozNym token panel hosted at IP address 204.155.31.133 using Victim 10's online banking credentials captured by GozNym malware, and attempted to cause two electronic funds transfers totaling $455,500.00 from Victim 10's PNC account to beneficiary accounts provided and controlled by conspirators.

(11) Victim 11

136. Victim 11 was a casino located in Gulfport, Mississippi.

137. On or about April 18, 2016, conspirators sent Victim 11's employee a phishing email and attachment designed to look legitimate, which enticed the employee to click on the

attachment and, in doing so, caused the installation of GozNym malware on Victim 11's computer.

138. On or about April 21, 2016, conspirators gained unauthorized access to Victim 11's People's Bank account using online banking login credentials captured by GozNym malware, and attempted to cause four electronic funds transfers totaling $197,300.00 from Victim 11's account to beneficiary bank accounts provided and controlled by the conspirators. One electronic funds transfer for $92,500.00 was destined for a beneficiary bank account ending in 2263 in the name Harris Insurance. A second transfer for $92,500.00 was destined for a beneficiary bank account ending in 3338 in the name Croulet and Associates.

139. On or about May 3, 2016, Krasimir Nikolov sent a message to ALEXANDER KONOVOLOV containing the details for the same beneficiary account ending in 2263 in the name Harris Insurance as well as the details for the same beneficiary account ending in 3338 in the name Croulet and Associates for which Victim 11's stolen funds were destined.

(12) Victim 12

140. Victim 12 was a stud farm located in Midway, Kentucky that specialized in breeding, selling, and racing thoroughbred horses.

141. On April 21, 2016, defendant ALEXANDER VAN HOOF, a/k/a "al666," provided a conspirator with detailed information regarding two beneficiary accounts designated to receive stolen funds from GozNym victims.

142. On or about April 21, 2016, conspirators gained unauthorized access to Victim 12's Limestone Bank account using online banking login credentials captured by GozNym malware, and attempted to cause three electronic funds transfers totaling $60,000.00, from Victim 12's account to beneficiary accounts provided and controlled by conspirators. In

particular, the two beneficiary accounts provided and controlled by VAN HOOF were designated to receive a total of $17,000.

(13) Victim 13

143. Victim 13 was a law office located in Wellesley, Massachusetts.

144. On or about August 30, 2016, Krasimir Nikolov gained unauthorized access to Victim 13's Brookline Bank account using online banking login credentials captured by GozNym malware, and attempted to cause, and did cause, an electronic funds transfer in the amount of $41,000.00 from Victim 13's account to a beneficiary account at TD Bank provided and controlled by a conspirator.

145. On or about August 30, 2016, Krasimir Nikolov provided the details of the electronic funds transfer, including the $41,000.00 amount and the name of the Victim 13's employee on the transfer, to the conspirator who provided and controlled the beneficiary account at TD Bank.

146. On or about September 2, 2016, Krasimir Nikolov communicated with MARAT KAZANDJIAN and ALEXANDER KONOLOLOV regarding the fraudulent $41,000.00 electronic funds transfer from Victim 13's bank account, as well as the agreed upon percentage split of the stolen funds amongst the conspirators. The fraudulent transaction resulted in a loss of $41,000.00.

All in violation of Title 18, United States Code, Section 371.

COUNT TWO
(Conspiracy to Commit Wire and Bank Fraud)

The grand jury further charges:

147. The allegations contained in Paragraphs 1 through 145 of this Indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

Statutory Allegations

148. From in and around October 2015, and continuing thereafter to in and around December 2016, in the Western District of Pennsylvania and elsewhere, the defendants, ALEXANDER KONOVOLOV, a/k/a "NoNe," a/k/a "none_1," MARAT KAZANDJIAN, a/k/a "phant0m," VLADIMIR GORIN, a/k/a "Voland," a/k/a "mrv," a/k/a "riddler," GENNADY KAPKANOV, a/k/a "Hennadiy Kapkanov," a/k/a "flux," a/k/a "ffhost," a/k/a "firestarter," a/k/a "User 41," KONSTANTIN VOLCHKOV, a/k/a "elvi," EDUARD MALANICI, a/k/a "JekaProf," a/k/a "procryptgroup," RUSLAN VLADIMIROVICH KATIRKIN, a/k/a "stratos," a/k/a "xen," VIKTOR VLADIMIROVICH EREMENKO, a/k/a "nfcorpi," FARKHAD RAUF OGLY MANOKHIN, a/k/a "frusa," ALEXANDER VAN HOOF, a/k/a "al666," along with conspirator Krasimir Nikolov, a/k/a "pablopicasso," a/k/a "salvadordali," a/k/a "karlo" knowingly and willfully did conspire, combine, and agree together and with other persons known and unknown to the grand jury to commit wire fraud and bank fraud, to wit:

a. to knowingly and willfully devise and execute, and attempt to execute, a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises; and in executing and attempting to execute this scheme and artifice, to knowingly cause to be transmitted in interstate and foreign commerce, by means of wire communication, certain signs, signals and sounds as further described herein, in violation of Title 18, United States Code, Section 1343;

b. to knowingly and willfully devise and execute, and attempt to execute, a scheme and artifice to defraud financial institutions, as defined in Title 18, United States Code, Section 20, and to obtain moneys and funds under the custody and control of financial institutions by means of materially false and

fraudulent pretenses, representations, and promises, in violation of Title 18, United States Code, Section 1344.

Objectives of the Conspiracy

149. The objectives of the conspiracy included: (a) infecting victims' computers with GozNym malware designed to capture victims' online banking login credentials; (b) using the captured login credentials to gain unauthorized access to victims' online bank accounts at U.S. financial institutions; and (c) stealing funds from victims' U.S. bank accounts and laundering those funds using U.S. and foreign beneficiary bank accounts provided and controlled by conspirators.

Manner and Means of the Conspiracy

150. The manner and means used to accomplish the objectives of the conspiracy are set forth in paragraphs 28 through 55 of this Indictment.

151. In order to infect victims' computer with GozNym malware, the defendants and conspirators known and unknown to the grand jury crafted and transmitted through the Internet in interstate and foreign commerce phishing emails containing malicious hyperlinks or attachments which, when clicked, downloaded GozNym malware onto victims' computers without the victims' knowledge or consent. The phishing emails were falsely designed to appear as legitimate business emails from companies and financial institutions in order to deceive victim recipients into opening the emails. The malicious hyperlinks and attachments were falsely represented to be legitimate links and attachments, such as business invoices, in order to fraudulently entice the victim recipients to click on them. GozNym malware captured the victims' online banking login credentials.

152. In order to fraudulently gain unauthorized access the victims' online bank accounts, the defendants, and conspirators known and unknown to the grand jury, used the

victims' captured online banking login credentials without authorization to falsely represent to banks that the defendants and their conspirators were victims or employees of victims who had authorization to access the bank accounts and to make electronic funds transfers from said accounts.

All in violation of Title 18, United States Code, Section 1349.

COUNT THREE

The grand jury further charges that:

153. The allegations contained in Paragraphs 1 through 145 of this Indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

154. From in and around October 2015, and continuing thereafter to in and around December 2016, in the Western District of Pennsylvania and elsewhere, the defendants, ALEXANDER KONOVOLOV, a/k/a "NoNe," a/k/a "none_1," MARAT KAZANDJIAN, a/k/a "phant0m," VLADIMIR GORIN, a/k/a "Voland," a/k/a "mrv," a/k/a "riddler," GENNADY KAPKANOV, a/k/a "Hennadiy Kapkanov," a/k/a "flux," a/k/a "ffhost," a/k/a "firestarter," a/k/a "User 41," KONSTANTIN VOLCHKOV, a/k/a "elvi," EDUARD MALANICI, a/k/a "JekaProf," a/k/a "procryptgroup," RUSLAN VLADIMIROVICH KATIRKIN, a/k/a "stratos," a/k/a "xen," VIKTOR VLADIMIROVICH EREMENKO, a/k/a "nfcorpi," FARKHAD RAUF OGLY MANOKHIN, a/k/a "frusa," and ALEXANDER VAN HOOF, a/k/a "al666," along with conspirator Krasimir Nikolov, a/k/a "pablopicasso," a/k/a "salvadordali," a/k/a "karlo," and others known and unknown to the grand jury, intentionally and knowingly did combine, conspire, and agree together and with each other to commit money laundering against the United States in violation of Title 18, United States Code, Sections 1956, that is:

a. to knowingly conduct and attempt to conduct financial transactions involving property representing the proceeds of specified unlawful activity, namely, computer fraud, in violation of Title 18, United States Code, Section 1030, knowing that the transactions were designed, in whole or in part, to conceal and disguise the nature, location, source, ownership and control of the proceeds of the specified unlawful activity, contrary to the provisions of Title 18, United States Code, Section 1956(a)(1)(B)(i);

b. to knowingly transport, transmit, transfer, and attempt to transport, transmit, and transfer funds from a place in the United States to a place outside the United States, knowing that the funds involved in the transportation, transmission, and transfer represent the proceeds of unlawful activity, namely, computer fraud, in violation of Title 18, United States Code, Section 1030,

and knowing that such transportation, transmission, and transfer is designed, in whole or in part, to conceal and disguise the nature, location, source, ownership and control of the proceeds of the unlawful activity, contrary to the provisions of Title 18, United States Code, Section 1956(a)(2)(B)(i);

Objectives of the Conspiracy

155. The objectives of the conspiracy included: (a) infecting victims' computers with GozNym malware designed to capture victims' online banking login credentials; (b) using the captured login credentials to gain unauthorized access to victims' online bank accounts at U.S. financial institutions; and (c) stealing funds from victims' U.S. bank accounts and laundering those funds using U.S. and foreign beneficiary bank accounts provided and controlled by conspirators.

Manner and Means of the Conspiracy

156. The manner and means used to accomplish the objectives of the conspiracy are set forth in paragraphs 28 through 55 of this Indictment.

157. The defendants, and conspirators known and unknown to the grand jury, did conduct and attempt to conduct unauthorized electronic funds transfers from victims' online bank accounts at U.S. financial institutions into U.S. and foreign beneficiary bank accounts provided and controlled by conspirators.

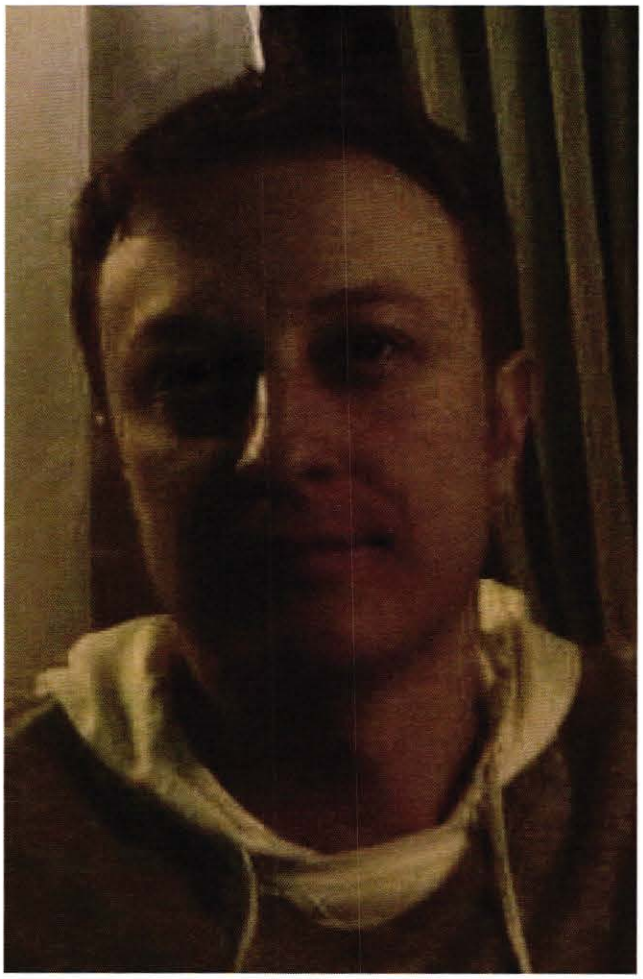
All in violation of Title 18, United States Code, Section 1956(h).

A True Bill,

[redacted]

FOREPERSON

SCOTT W. BRADY
United States Attorney
PA ID No. 88352

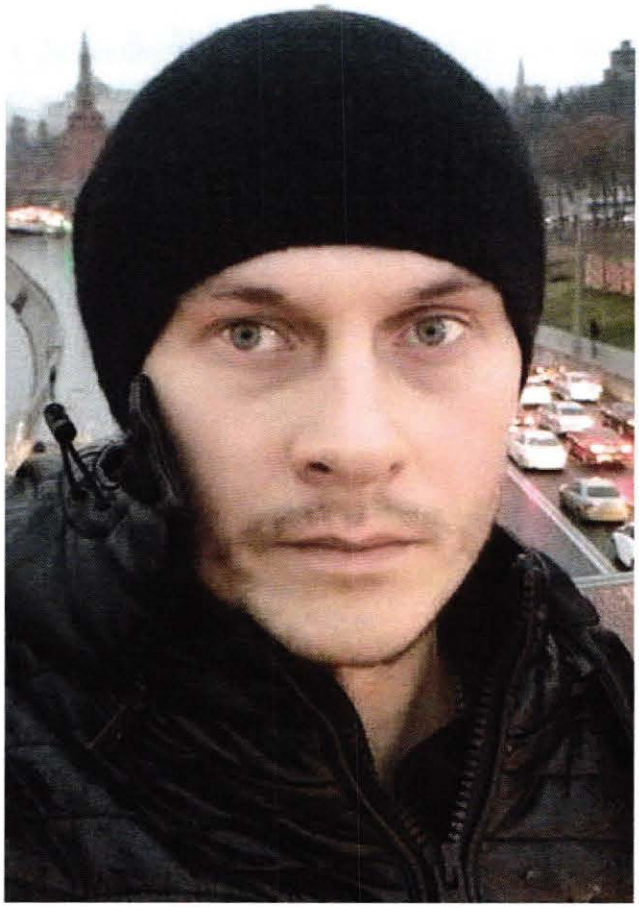


Alexander Konovolov

Exhibit A

Marat Kazandjian

Exhibit B



Vladimir Gorin

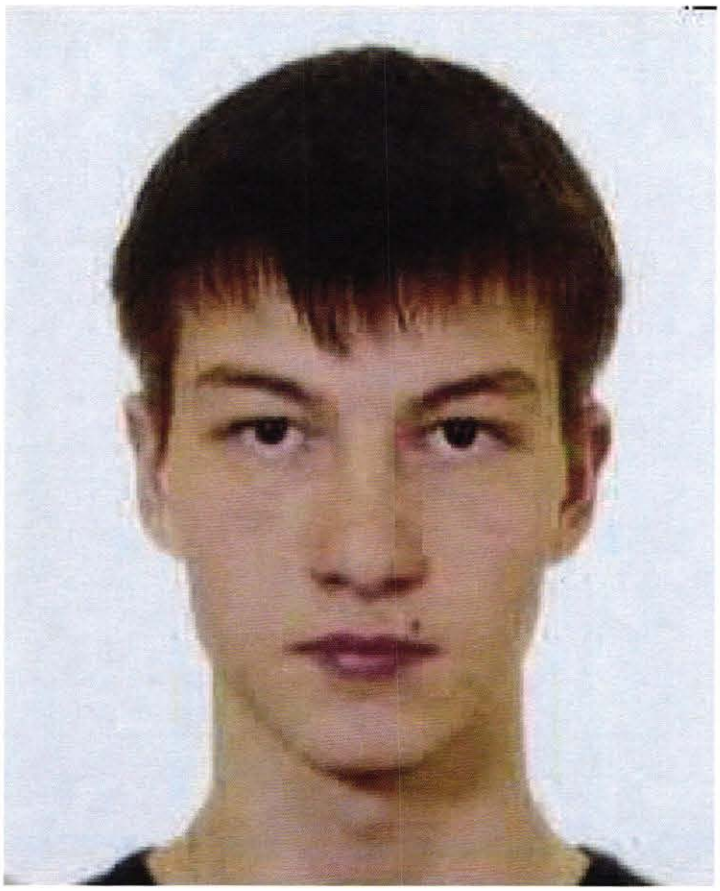
Exhibit C

Gennady Kapkanov

Exhibit D

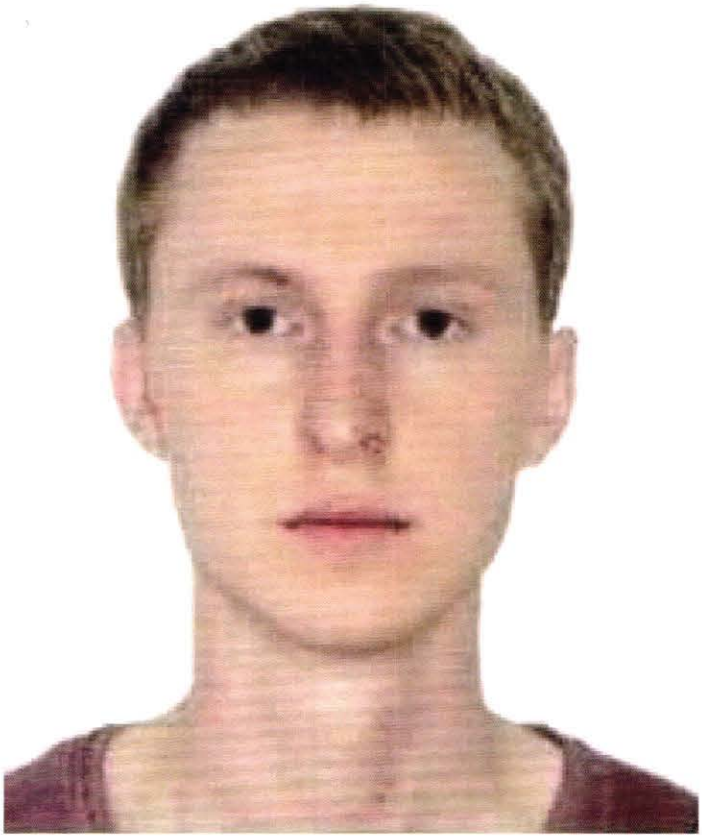
Eduard Malanici

Exhibit E



Ruslan Vladimirovich Katirkin

Exhibit F

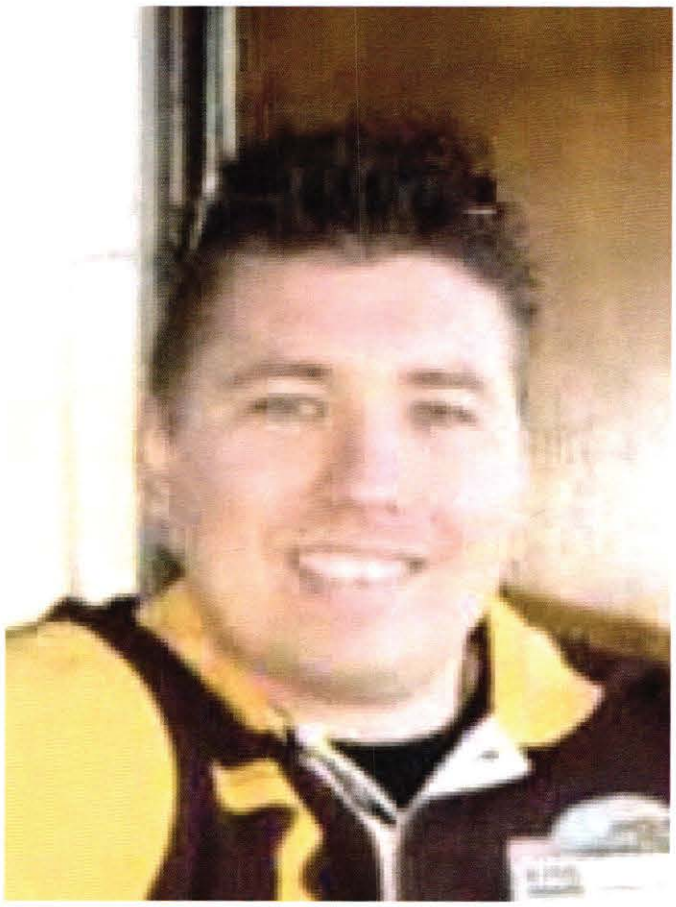


Viktor Vladimirovich Eremenko

Exhibit G

Farkhad Rauf Ogly Manokhin

Exhibit H



Alexander Van Hoof

Exhibit I

Абузоустойчивые решения: fast flux, сервера/VPS, проксирование, домены/SSL

10.11.2014, 16:42 #1

user41
Vendor of: hosting

user41 is offline
Join Date: 31.05.2011
Posts: 29
Deposit: 400$?
Trust Limit: 0$?

Абузоустойчивые решения: fast flux, сервера/VPS, проксирование, домены/SSL

Здравствуйте!

Предлагаем Вам следующие услуги:

- **Абузоустойчивый хостинг по технологии Fast Flux** (хостинг на ботах) под любые проекты. Боты отбираются исключительно на высокоскоростных каналах. Хостинг имеет стабильно высокий аптайм.

- **Редиректы (проксирование) с поддержкой https/SSL.** Идеально подходит для владельцев ботнетов, благодаря такой технологии все абузы будут оставаться у нас. Что позволит Вам использовать сервер в любом дата центре.

- **Абузоустойчивые выделенные сервера и VPS.** С возможностью держать абузы от спамхауза.

- **Регистрация доменов и SSL сертификатов.**

Действуют системы скидок и бонусов.

По всем вопросам обращаться в jabber: **flux@jabber-im.net** или **flux2@jabber-im.net**

Абузоустойчивые решения: fast flux, сервера/VPS, проксирование, домены/SSL

Exhibit J

QUOTE

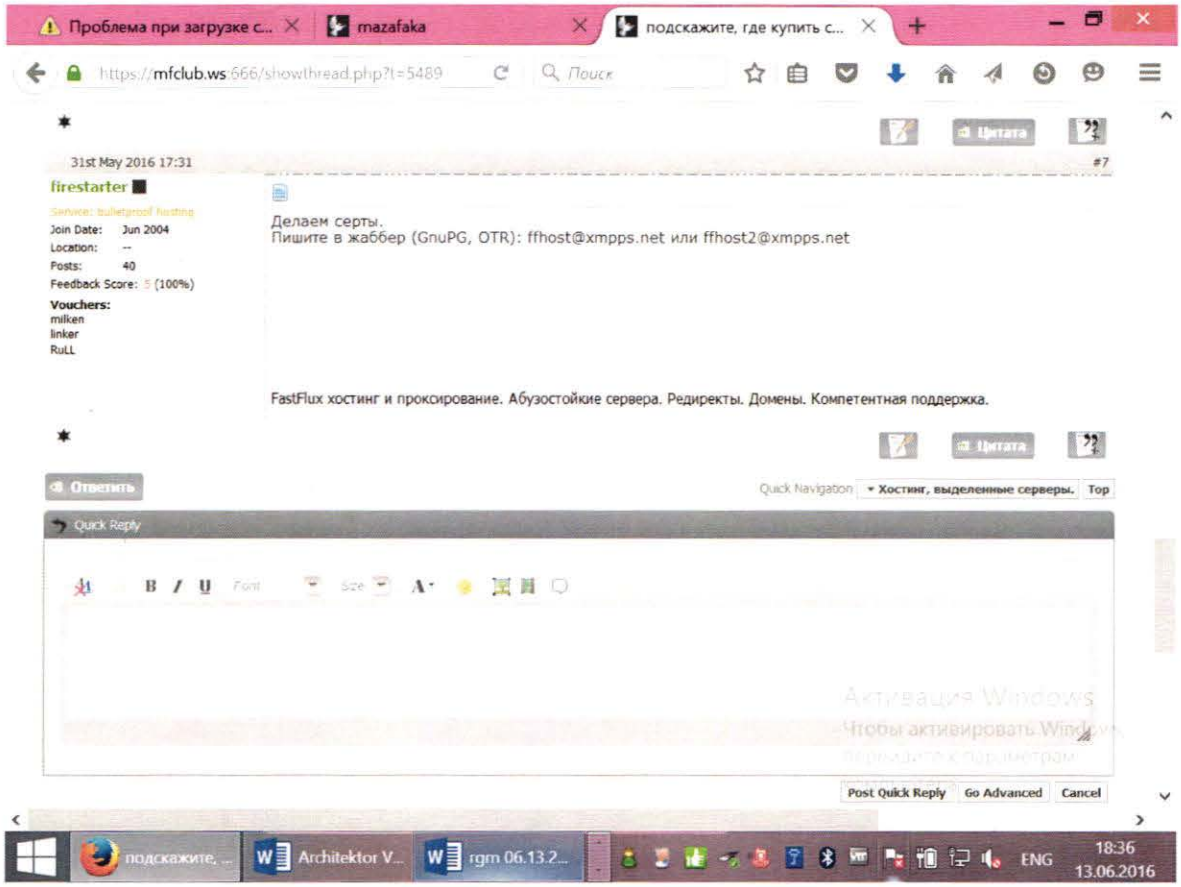

Проблема при загрузке с...
mazafaka
подскажите, где купить с...
https://mfclub.ws:666/showthread.php?t=5489
Поиск
Цитата
31st May 2016 17:31
#7
firestarter
Service: bulletproof hosting
Join Date: Jun 2004
Location: --
Posts: 40
Feedback Score: 5 (100%)
Vouchers:
milken
linker
RuLL
Делаем серты.
Пишите в жаббер (GnuPG, OTR): ffhost@xmpps.net или ffhost2@xmpps.net
FastFlux хостинг и проксирование. Абузостойкие сервера. Редиректы. Домены. Компетентная поддержка.
Цитата
Ответить
Quick Navigation
Хостинг, выделенные серверы.
Top
Quick Reply
Font
Size
Активация Windows
Чтобы активировать Windows
Post Quick Reply
Go Advanced
Cancel
подскажите, ...
Architektor V...
rgm 06.13.2...
ENG
18:36
13.06.2016

Exhibit K

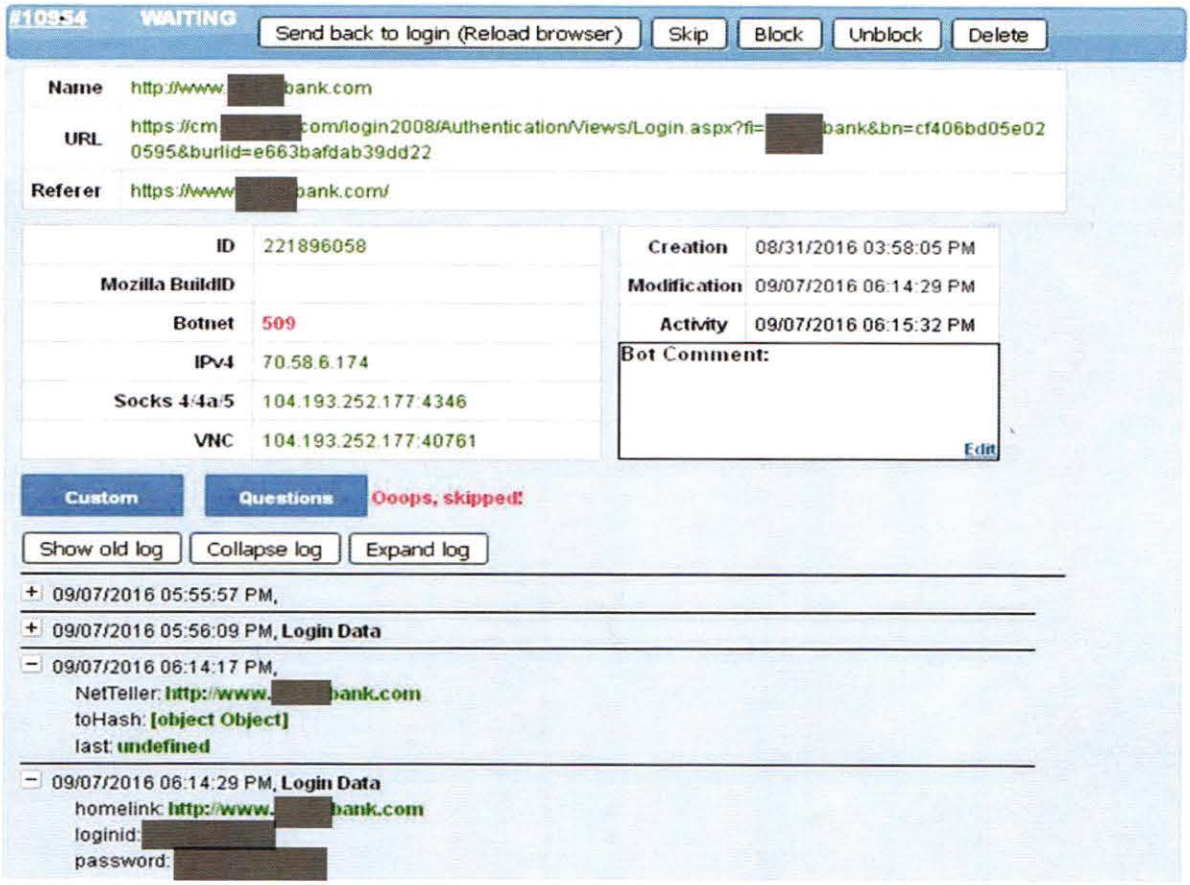

#10854 WAITING
Send back to login (Reload browser)
Skip
Block
Unblock
Delete
Name http://www.[redacted]bank.com
URL https://cm[redacted]com/login2008/Authentication/Views/Login.aspx?fi=[redacted]bank&bn=cf406bd05e020595&burlid=e663bafdab39dd22
Referer https://www[redacted]bank.com/
ID 221896058
Mozilla BuildID
Botnet 509
IPv4 70.58.6.174
Socks 4/4a/5 104.193.252.177:4346
VNC 104.193.252.177:40761
Creation 08/31/2016 03:58:05 PM
Modification 09/07/2016 06:14:29 PM
Activity 09/07/2016 06:15:32 PM
Bot Comment:
Edit
Custom
Questions
Ooops, skipped!
Show old log
Collapse log
Expand log
+ 09/07/2016 05:55:57 PM,
+ 09/07/2016 05:56:09 PM, Login Data
- 09/07/2016 06:14:17 PM,
NetTeller: http://www.[redacted]bank.com
toHash: [object Object]
last: undefined
- 09/07/2016 06:14:29 PM, Login Data
homelink: http://www.[redacted]bank.com
loginid: [redacted]
password: [redacted]

Exhibit L

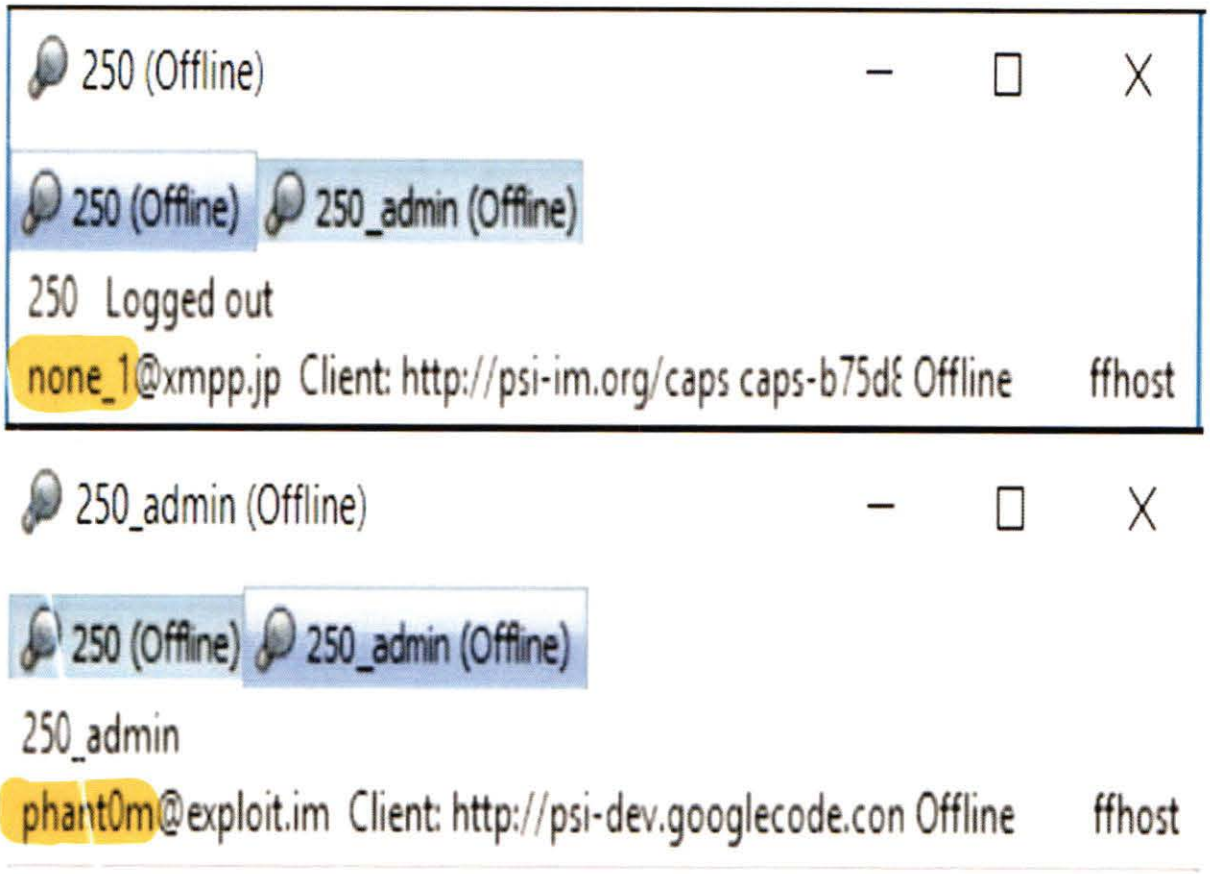

250 (Offline)
250 (Offline)
250_admin (Offline)
250 Logged out
none_1@xmpp.jp Client: http://psi-im.org/caps caps-b75d8 Offline ffhost
250_admin (Offline)
250 (Offline)
250_admin (Offline)
250_admin
phant0m@exploit.im Client: http://psi-dev.googlecode.con Offline ffhost

Exhibit M

3248	2949	2016-01-18 10:39:11	forget42gibb.com	38	7	ns1.mommefubsy.pw ns1.hippaculpa.p
3249	2950	2016-01-18 10:39:53	grotesk14file.com	38	5	ns1.mommefubsy.pw ns2.mommefubs
3250	2951	2016-01-18 10:50:22	finn4kbimm.com	38	4	ns1.google.com ns2.google.com
3251	2976	2016-01-23 11:29:52	finiki45toget.com	38	5	ns1.mommefubsy.pw ns1.hippaculpa.p
3252	2977	2016-01-23 11:35:58	joreshi50indo.com	38	7	ns1.mommefubsy.pw ns1.hippaculpa.p
3253	2988	2016-01-25 11:09:07	epay-solution.com	38	5	ns1.mommefubsy.pw ns1.hippaculpa.p
3254	3198	2016-02-16 07:02:34	billpay-center.com	38	4	ns1.google.com ns2.google.com
3255	3228	2016-02-21 16:42:54	amoretanointrodano31.com	38	4	ns1.kasmpudge.pw ns2.kasmpudge.pw

Exhibit N

From: [redacted]
Sent: Thursday, February 18, 2016 10:51 AM
To: [redacted]
Subject: Bank of America

Bank of America

Good morning,

Please see the attached invoice and remit payment according to the terms listed at the bottom of the invoice. If you have any questions please let us know.

Thank you!

Mr. [redacted] J.D.
Accounting Specialist| Bank of America, [redacted] PLLC

invoice_0028556.doc

Exhibit O

[2/16/2016 7:45:02 AM] 250:
<GPGdec>rassilka 4erez fustflux doc macrosda v tele pisem budet to4e4no na jertv slatsa link</GPGdec>

[2/16/2016 7:45:28 AM] 250:
<GPGdec>http://www.billpay-center.com/invoice#007448322.doc</GPGdec>

[2/16/2016 7:45:31 AM] 250:
<GPGdec>kak to tak</GPGdec>

[2/16/2016 7:45:35 AM] 250:
<GPGdec>no nebolshoe kol-vo</GPGdec>

[2/16/2016 7:45:37 AM] 250:
<GPGdec>1k botov</GPGdec>

[2/16/2016 7:46:27 AM] ffhost:
окей
ну как я и говорил выше - домен можем сделать, но гарантий дать не могу т.к. всё очень относительно

[2/16/2016 7:46:42 AM] 250:
<GPGdec>ok</GPGdec>

[2/16/2016 7:46:56 AM] 250:
<GPGdec>billpay-center.com</GPGdec>

[2/16/2016 7:46:59 AM] 250:
<GPGdec>posmotri svoboden</GPGdec>

Exhibit P

Milochik, Michael (MPD)

From: [redacted]

Sent: Tuesday, February 16, 2016 10:59 AM
To: [redacted]
Subject: Your Quicken Bill Pay Invoice from 02/12/2016.

Greetings from Quicken Billpay-center!

Thank you for your business, and we look forward to the opportunity of serving you again in the future.

Click the link below to view your Invoice.

http://www.billpay-center.com/invoices/007448322.doc

If you have any questions call us at 1-877-488-8843.

Sincerely,
Billpay-center

This message has been scanned for viruses and dangerous content by MailScanner, and is believed to be clean.

Exhibit Q

From: [redacted]
Sent: 2/22/2016 4:35:34 PM +0000
To: [redacted]
Subject: Bank of America Payment

Bank of America

Good morning,

Please see the attached invoice and remit payment according to the terms listed at the bottom of the you have any questions please let us know

Invoice_897-84579.doc

Thank you!

Mr [redacted] J.D.
Accounting Specialist| Bank of America [redacted] PLLC

Exhibit R