United States District Court

FOR THE
NORTHERN DISTRICT OF CALIFORNIA

VENUE: SAN FRANCISCO

FILED
2017 FEB 28 P 1:50
SUSAN Y. SOONG
CLERK, US DISTRICT COURT
NO. DIST. OF CA.

UNITED STATES OF AMERICA,

V.

SEALED
BY COURT ORDER

DMITRY DOKUCHAEV, a/k/a "Patrick Nagel," IGOR SUSHCHIN, ALEXSEY BELAN, a/k/a "Magg," and KARIM BARATOV, a/k/a "Kay," a/k/a "Karim Taloverov," a/k/a "Karim Akehmet Tokbergenov

VC

CR17 108

DEFENDANT(S).

INDICTMENT

18 U.S.C. § 1030(b) – Conspiracy To Commit Computer Fraud And Abuse; 18 U.S.C. § 1831(a)(5) – Conspiracy To Commit Economic Espionage; 18 U.S.C. § 1832(a)(5) – Conspiracy to Steal Trade Secrets; 18 U.S.C. § 1831(a)(1) – Economic Espionage; 18 U.S.C. § 1832(a)(1) – Theft of Trade Secrets; 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud; 18 U.S.C. § 1030(a)(2)(C) – Unauthorized Access to Protected Computers; 18 U.S.C. § 1030(a)(5)(A) – Damaging Protected Computers; 18 U.S.C. § 1029(b)(2) – Conspiracy to Commit Fraud in Connection with Access Devices; 18 U.S.C. § 1030(a)(2)(C) – Unauthorized Access to Protected Computers; 18 U.S.C. § 1029(a)(1) – Trafficking in Counterfeit Access Devices; 18 U.S.C. § 1028A – Aggravated Identity Theft; 18 U.S.C. § § 982(a)(2)(B) & 1030(i) and (j) – First Forfeiture Allegation; 18 U.S.C. § § 1834 and 2323 – Second Forfeiture Allegation; 18 U.S.C. § §981(a)(1)(C), 982(a)(2)(B) and 1029(c)(1)(C) and 28 U.S.C. § 2461(c) – Third Forfeiture Allegation.

A true bill.

[redacted]

Foreman

Filed in open court this 28th day of

Feb, 2017

Clerk

Bail, $ no bail for all defendants

Laurel Beeler
United States Magistrate Judge

BRIAN J. STRETCH (CABN 163973)
United States Attorney

FILED
2017 FEB 28 P 1:50
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NO. DIST. OF CA.

SEALED
BY COURT ORDER

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

VC

SAN FRANCISCO DIVISION

CR17 103

UNITED STATES OF AMERICA,

Plaintiff,

v.

DMITRY DOKUCHAEV,
a/k/a "Patrick Nagel"
IGOR SUSHCHIN,
ALEXSEY BELAN,
a/k/a "Magg"
and
KARIM BARATOV
a/k/a "Kay"
a/k/a "Karim Taloverov"
a/k/a "Karim Akehmet Tokbergenov"

Defendants.

UNDER SEAL

VIOLATIONS:
18 U.S.C. § 1030(b) – Conspiracy To Commit Computer Fraud And Abuse; 18 U.S.C. § 1831(a)(5) – Conspiracy To Commit Economic Espionage; 18 U.S.C. § 1832(a)(5) – Conspiracy to Steal Trade Secrets; 18 U.S.C. § 1831(a)(1) – Economic Espionage; 18 U.S.C. § 1832(a)(1) – Theft of Trade Secrets; 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud; 18 U.S.C. § 1030(a)(2)(C) – Unauthorized Access to Protected Computers; 18 U.S.C. § 1030(a)(5)(A) – Damaging Protected Computers; 18 U.S.C. § 1029(b)(2) – Conspiracy to Commit Fraud in Connection with Access Devices; 18 U.S.C. § 1030(a)(2)(C) – Unauthorized Access to Protected Computers; 18 U.S.C. § 1029(a)(1) – Trafficking in Counterfeit Access Devices; 18 U.S.C. § 1028A – Aggravated Identity Theft; 18 U.S.C. § § 982(a)(2)(B) & 1030(i) and (j) – First Forfeiture Allegation; 18 U.S.C. § § 1834 and 2323 – Second Forfeiture Allegation; 18 U.S.C. § §981(a)(1)(C), 982(a)(2)(B) and 1029(c)(1)(C) and 28 U.S.C. § 2461(c) – Third Forfeiture Allegation

INDICTMENT

The Grand Jury charges—

At all times relevant to this Indictment, unless otherwise stated:

INTRODUCTION

1. From at least in or about 2014 up to and including at least in or about December 2016, officers of the Russian Federal Security Service ("FSB"), an intelligence and law enforcement agency of the Russian Federation ("Russia") headquartered in Lubyanka Square, Moscow, Russia, and a successor service to the Soviet Union's Committee of State Security ("KGB"), conspired together and with each other to protect, direct, facilitate, and pay criminal hackers to collect information through computer intrusions in the United States and elsewhere. The FSB officers, defendants DMITRY DOKUCHAEV, IGOR SUSHCHIN, and others known and unknown to the Grand Jury, directed the criminal hackers, defendants ALEXSEY BELAN, KARIM BARATOV, and others known and unknown to the Grand Jury (collectively, the "conspirators"), to gain unauthorized access to the computers of companies providing webmail and internet-related services located in the Northern District of California and elsewhere, to maintain unauthorized access to those computers, and to steal information from those computers, including information regarding, and communications of, the providers' users.

2. In some cases, the conspirators sought unauthorized access to information of predictable interest to the FSB. For example, as described in more detail below, the conspirators sought access to the Yahoo, Inc. ("Yahoo") email accounts of Russian journalists; Russian and U.S. government officials; employees of a prominent Russian cybersecurity company; and numerous employees of U.S., Russian, and other foreign webmail and internet-related service providers whose networks the conspirators sought to further exploit.

3. In other cases, the conspirators sought access to accounts of employees of commercial entities, including executives and other managers of a prominent Russian investment banking firm (the "Russian Financial Firm"); a French transportation company; U.S. financial services and private equity firms; a Swiss bitcoin wallet and banking firm; and a U.S. airline.

4. One of the criminal hackers, BELAN, has been the subject of an Interpol "Red Notice" and listed as one of the Federal Bureau of Investigation's ("FBI") "Most Wanted" hackers since 2012. BELAN resides in Russia, within the FSB's jurisdiction to arrest and prosecute. Rather than arrest him, however, the FSB officers used him. They also provided him with sensitive FSB law enforcement and intelligence information that would have helped him avoid detection by law enforcement, including

information regarding FSB investigations of computer hacking and FSB techniques for identifying criminal hackers. It was BELAN who provided his FSB conspirators, including DOKUCHAEV and SUSHCHIN, with the unauthorized access to Yahoo's network described above.

5. In addition to executing DOKUCHAEV and SUSHCHIN's taskings, BELAN leveraged his access to Yahoo's network to enrich himself: (a) through an online marketing scheme, by manipulating Yahoo search results for erectile dysfunction drugs; (b) by searching Yahoo user email accounts for credit card and gift card account numbers and other information that could be monetized; and (c) by gaining unauthorized access to the accounts of more than 30 million Yahoo users, the contacts of whom were then stolen as part of a spam marketing scheme.

6. When the FSB officers, SUSHCHIN and DOKUCHAEV, learned that a target of interest had email accounts at webmail providers other than Yahoo, including through information gained from the Yahoo intrusion, they would task BARATOV to access the target's account at the other providers. When BARATOV was successful, as was often the case, his handling FSB officer, DOKUCHAEV, paid him a bounty.

7. For example, SUSHCHIN, DOKUCHAEV, and BARATOV sought access to the Google, Inc. ("Google") webmail accounts of:

a. an assistant to the Deputy Chairman of the Russian Federation;

b. an officer of the Russian Ministry of Internal Affairs;

c. a physical training expert working in the Ministry of Sports of a Russian republic; and

d. others, including additional examples described below.

THE DEFENDANTS

8. DMITRY ALEKSANDROVICH DOKUCHAEV, also known as "Patrick Nagel," was a Russian national and resident. DOKUCHAEV was an FSB officer assigned to Second Division of FSB Center 18, also known as the FSB Center for Information Security. He was an associate of FSB officer IGOR SUSHCHIN; another, supervisory FSB officer known to the Grand Jury ("FSB Officer 3"), who was the senior FSB official assigned to Center 18; and other FSB officers known and unknown. DOKUCHAEV's photograph is attached as Exhibit A.

9. IGOR ANATOLYEVICH SUSHCHIN was a Russian national and resident. SUSHCHIN was an FSB officer, and DOKUCHAEV's superior within the FSB. SUSHCHIN was also an associate of FSB Officer 3, and other FSB officers known and unknown. SUSHCHIN was embedded as a purported employee and Head of Information Security at the Russian Financial Firm, where he monitored the communications of Russian Financial Firm employees, although it is unknown to the grand jury whether the Russian Financial Firm knew of his FSB affiliation. SUSHCHIN's photograph is attached as Exhibit B.

10. ALEXSEY ALEXSEYEVICH BELAN, also known as "Magg," was a Russian national and resident. He was a criminal hacker and associate of DOKUCHAEV. BELAN assisted DOKUCHAEV by carrying out hacking assignments. BELAN was indicted in September 2012 in the District of Nevada for computer fraud and abuse and related crimes in connection with his intrusion into the computer systems of a U.S. e-commerce company. He was also indicted in June 2013 in the Northern District of California for computer fraud and abuse and related crimes in connection with intrusions at two other U.S. e-commerce companies. He was arrested in 2013 in a European country on a U.S. provisional arrest warrant, but before he could be extradited to the United States, he was able to leave that country and return to Russia. Currently, BELAN is the subject of an outstanding Interpol "Red Notice" requesting that Interpol member nations (including Russia) arrest and extradite him. BELAN is also on the FBI's list of "Most Wanted" hackers and was recently the subject of the December 29, 2016 sanctions designation by the President of the United States based, at least in part, on his "significant malicious cyber-enabled misappropriation of personal identifiers for private financial gain" in relation to the above-described criminal charges. BELAN's photograph is attached as Exhibit C.

11. KARIM BARATOV, also known as "Kay," "Karim Taloverov" and "Karim Akehmet Tokbergenov," was a Canadian national and resident. He was a criminal hacker and associate of DOKUCHAEV. BARATOV assisted DOKUCHAEV by carrying out his hacking assignments. BARATOV's photograph is attached as Exhibit D.

COUNT ONE: 18 U.S.C. § 1030(b) – Conspiracy to Commit Computer Fraud and Abuse

12. Paragraphs 1 through 11 of this Indictment are hereby re-alleged and incorporated by reference as if set forth in full herein.

13. From a date unknown to the Grand Jury, but no later than January 2014, and continuing through December 1, 2016, in the Northern District of California and elsewhere, the defendants

DMITRY DOKUCHAEV,
ALEXSEY BELAN,
IGOR SUSHCHIN, and
KARIM BARATOV,

did knowingly and willfully conspire and agree with each other, and with others known and unknown to the Grand Jury, to commit computer fraud and abuse, namely:

a. to access computers without authorization and exceed authorized access to computers, in the Northern District of California and elsewhere, and to thereby obtain information from protected computers, for the purpose of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the laws of California, including invasion of privacy, and where the value of the information did, and would if completed, exceed $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(i)-(iii); and

b. to cause the transmission of programs, information, codes, and commands, in the Northern District of California and elsewhere, and as a result of such conduct, to cause damage without authorization to protected computers, and where the offense did cause and would, if completed, have caused, loss aggregating $5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, and damage affecting at least 10 protected computers during a one-year period, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B).

MANNER AND MEANS OF THE CONSPIRACY

14. The conspirators used the following manner and means to accomplish their objectives.

15. The conspirators, directly and through intermediaries, attempted to hide the nature and origin of their internet traffic and reduce the likelihood of detection by victims and law enforcement, by

leasing servers in numerous countries, including the United States, and using other services like virtual private networks.

16. The conspirators used numerous email accounts hosted by webmail providers in the United States and elsewhere, including Russia, which they often registered using false subscriber information.

17. In some instances, the conspirators used email messages known as "spear phishing" messages to trick unwilling recipients into giving the co-conspirators access to their computers and accounts. Spear phishing messages typically were designed to resemble emails from trustworthy senders, and to encourage the recipient to open attached files or click on hyperlinks in the messages. Some spear phishing emails attached or linked to files that, once opened or downloaded, installed "malware"—malicious code or programs—that provided unauthorized access to the recipient's computer (a "backdoor"). Other spear phishing emails lured the recipient into providing valid login credentials to his or her account(s), thereby allowing the defendants to bypass normal authentication procedures.

18. In many instances, the conspirators engaged in the manual creation of account authentication "cookies," known as "minting," to gain unauthorized access to victim webmail accounts. Cookies are small files stored on a user's computer by the user's web browser. Upon a user's connection to a webmail server, the server can read the data in the cookie and obtain information about that specific user. Among other uses, cookies enable webmail providers to recognize an account user who had previously logged into his or her account, and to allow that user, for a specified duration, to continue to access the account's contents without re-entering his or her password.

19. The conspirators frequently sought unauthorized access to the email accounts of close associates of their intended victims, including spouses and children, to gain additional information about and belonging to their intended victims.

The Yahoo Intrusions

20. Yahoo was a webmail provider based in Sunnyvale, California, which provided internet services, including electronic messaging services, to more than 1 billion users.

21. Beginning no later than 2014, the conspirators stole non-content information regarding more than 500 million Yahoo user accounts as a result of their malicious intrusion. The theft of user data was part of a larger intrusion into Yahoo's computer network, which continued to and including at least September 2016. As part of this intrusion, malicious files and software tools were downloaded onto Yahoo's computer network, and used to gain and maintain further unauthorized access to Yahoo's network and to conceal the extent of such access.

22. The user data referenced in the preceding paragraph was held in Yahoo's User Database ("UDB"). The UDB was, and contained, proprietary and confidential Yahoo technology and information, including, among other data, subscriber information, such as: account users' names; recovery email accounts and phone numbers, which users provide to webmail providers, such as Yahoo, as alternative means of communication with the provider; password challenge questions and answers; and certain cryptographic security information associated with the account, *i.e.* the account's "nonce", further described below. Some of the information in the UDB was stored in an encrypted form.

23. Yahoo used its Account Management Tool ("AMT") to access and edit the information stored in the UDB. The AMT allowed Yahoo to manage aspects of its users' accounts, including to make, log, and track changes to the account, such as password changes. The AMT was, and contained, proprietary and confidential Yahoo technology and information.

24. In or around early 2014, the conspirators gained unauthorized access to Yahoo's network and began their reconnaissance. After gaining unauthorized access to Yahoo's network, BELAN located relevant Yahoo network resources of interest, including the UDB and AMT.

25. In or around November and December 2014, BELAN stole a backup copy of the UDB as it existed in early November 2014. He removed at least some of the UDB copy to one of the computers under his control (the "BELAN Computer") by using the File Transfer Protocol, a common means of transferring data between computers.

26. Beginning in or around October 2014 and until at least November 2016, the conspirators accessed user account information and contents using a combination of methods, including without limitation: (a) via unauthorized access to Yahoo's AMT; (b) via the minting of authentication cookies on Yahoo's network to gain unauthorized access to victim webmail accounts; and (c) via the minting of authentication cookies outside Yahoo's network.

27. The conspirators minted authentication cookies "internally", *i.e.* within Yahoo's network, while they trespassed on the network. In order to mint cookies internally, the conspirators caused programs to be loaded onto Yahoo's network and computers without authorization.

28. The conspirators also minted authentication cookies "externally", *i.e.* outside Yahoo's network. In order to mint cookies externally, the conspirators required, among other information, a cryptographic value unique to the targeted victim account, called a "nonce." The nonces associated with individual Yahoo user accounts were stored in the UDB, and thus when BELAN stole a copy of at least a portion of the UDB in November and December 2014, the defendants obtained the nonces associated with affected user accounts.

29. Whenever a Yahoo user changed his or her password, the nonce associated with the account changed as well. As a result, comparing the date that victims last changed their passwords to the defendants' cookie minting attempts confirms that the conspirators employed the UDB copy that BELAN stole—*i.e.*, the UDB as it existed in early November 2014—to gain unauthorized access to Yahoo user accounts via external cookie minting. The conspirators failed to access those accounts whose users had changed their passwords after BELAN stole the UDB copy; but they succeeded in accessing those accounts that retained the same passwords in use at the time the conspirators obtained the UDB copy, including those accounts for which the user had most recently changed the password immediately prior to BELAN's theft of the UDB copy.

30. The conspirators discussed among themselves how to mint cookies to access Yahoo accounts. For example, on or about July 20, 2015, DOKUCHAEV sent SUSHCHIN a minted cookie for

a Yahoo user account, a file containing the below screenshot of a cookie manager application, and instructions for using the application to access the Yahoo email account.

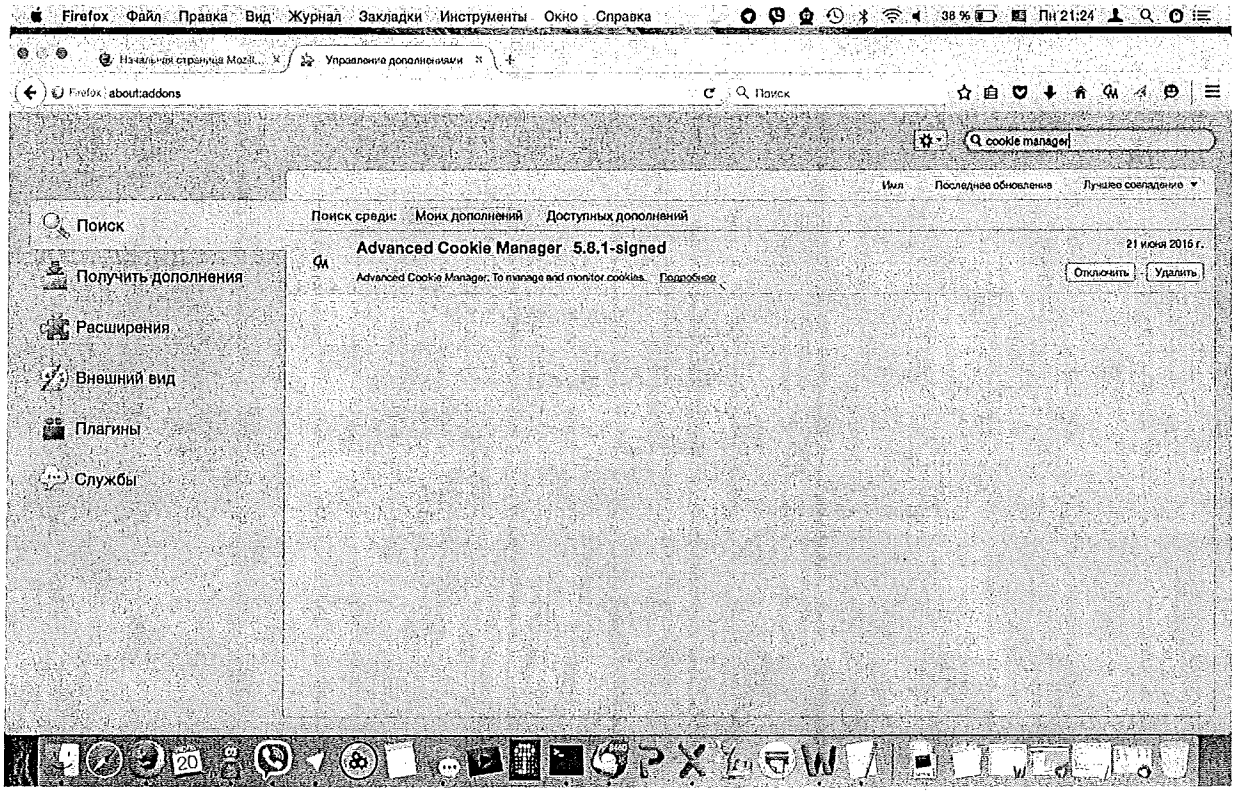

Figure 1: Screenshot of a cookie manager application

31. Both internally and externally minted cookies allowed the conspirators to appear to Yahoo's servers as if the intruder had previously obtained valid access to the associated Yahoo user's account, obviating the need to enter a username and password for that account. The conspirators utilized cookie minting to access the contents of more than 6,500 Yahoo user accounts.

32. The conspirators used their access to the AMT to (among other unauthorized actions) maintain persistent unauthorized access to some of the compromised accounts.

33. The AMT did not permit text searches of underlying data. It permitted the conspirators to access information about particular Yahoo user accounts. However, by combining their control of the stolen UDB copy and access to the AMT, the conspirators could, for example, search the UDB contents to identify Yahoo user accounts for which the user had provided a recovery email account hosted by a specific company of interest to the conspirators (*e.g.*, "exampleuser@ExampleCompany.com")—showing that the user was likely an employee of the company of interest—and then use information

from the AMT to gain unauthorized access to the identified accounts using the means described in paragraph 26.

34. The conspirators used their unauthorized access to Yahoo's network to identify and access accounts of, among other victims, users affiliated with U.S. online service providers, including but not limited to webmail providers and cloud computing companies, whose account contents could facilitate unauthorized access to other victim accounts; Russian journalists and politicians critical of the Russian government; Russian citizens and government officials; former officials from countries bordering Russia; and U.S. government officials, including cyber security, diplomatic, military, and White House personnel. For example:

a. In or around October 2014, the conspirators sought, and DOKUCHAEV later obtained, access to an account of a diplomat from a country bordering Russia who was posted in a European country.

b. From at least in or around December 2015 until May 2016, the conspirators sought access to accounts of the former Minister of Economic Development of a country bordering Russia ("Victim A") and his wife ("Victim B"). DOKUCHAEV, SUSHCHIN, and BELAN worked with FSB Officer 3 to access Victims A and B's accounts by minting cookies and to share information obtained from those accounts. In one instance, on or about December 18, 2015, FSB Officer 3 provided SUSHCHIN with information regarding a company controlled by Victims A and B. On or about December 21, 2015, DOKUCHAEV sent a cookie for Victim B's account to SUSHCHIN, who then later that day sent DOKUCHAEV a report on Victims A and B. On or about May 20, 2016, BELAN minted a cookie for the same Victim B account.

c. In or around December 2015 and January 2016, the conspirators sought access to an account of a Russian journalist and investigative reporter who worked for Kommersant Daily. DOKUCHAEV obtained information about the victim's account from the AMT and then obtained full access to the victim user's account by minting cookies on or about December 6, 2015, and January 21, 2016.

d. In or around December 2015 and January 2016, the conspirators sought access to an account of a public affairs consultant and researcher who analyzed Russia's bid for World Trade Organization membership. DOKUCHAEV accessed the contents of the victim user's account by minting cookies.

e. In or around February 2016, the conspirators sought access to Yahoo accounts of employees of a U.S. cloud storage company's ("U.S. Cloud Computing Company 1"). On or about February 26, 2016, DOKUCHAEV gained accessed to the Yahoo user accounts of three different officers of U.S. Cloud Computing Company 1, in each case by minting cookies.

f. In or around March 2016, the conspirators sought access to an account of a Russian Deputy Consul General. On or about March 19, 2016, DOKUCHAEV successfully minted a cookie to gain access to the victim's account.

g. In or around April 2016, the conspirators sought access to an account of a senior officer at a Russian webmail and internet-related services provider (the "Russian Webmail Provider"). On or about April 25, 2016, DOKUCHAEV successfully minted a cookie to gain access to the victim user's account.

35. The conspirators used their unauthorized access to Yahoo's network in order to defraud Yahoo users as well. For a period in or around November 2014, at around the same time he was working to provide DOKUCHAEV and SUSHCHIN with access to Yahoo's network, BELAN manipulated some of the servers associated with Yahoo's English-language search engine so that when users searched for erectile dysfunction medications, they were presented with a fraudulent link created by BELAN. When a Yahoo user clicked on that link, he or she was taken to the website of a U.S.-based cloud computing firm, U.S. Cloud Computing Company 2. The Yahoo search engine users were then automatically redirected, by malicious code placed by BELAN on the website of U.S. Cloud Computing Company 2, and without themselves taking any additional actions, to the website of an online pharmacy company. That online pharmacy company's marketing program paid commissions to marketers who successfully drove traffic to its website. As a result, BELAN was paid for diverting Yahoo search engine users to it.

36. Other examples of Yahoo users whose accounts the conspirators targeted and compromised include:

a. On or about July 11, 2015, BELAN gained access to accounts belonging to 14 employees of a Swiss bitcoin wallet and banking firm.

b. On or about February 13, 2016, one conspirator gained access to an account belonging to a sales manager at a major U.S. financial company.

c. On or about March 30, 2016, DOKUCHAEV gained access to an account belonging to a Nevada gaming official.

d. On or about April 14, 2016, BELAN gained access to an account belonging to a senior officer of a major U.S. airline.

e. On or about June 20, 2016, a defendant gained access to an account belonging to a Shanghai-based managing director of a U.S. private equity firm.

f. On or about October 22, 2016, the conspirators gained access to accounts of the Chief Technology Officer of a French transportation company.

g. The conspirators sought access to accounts of multiple Yahoo users affiliated with the Russian Financial Firm. In one instance, in or around April 2015, SUSHCHIN ordered DOKUCHAEV to target a number of individuals, including a senior board member of the Russian Financial Firm, his wife, and his secretary; and a senior officer of the Russian Financial Firm ("Corporate Officer 1"). In or around April 2015, the conspirators gained access to a Yahoo account the conspirators mistakenly believed belonged to Corporate Officer 1. In or around October 2015, SUSHCHIN and DOKUCHAEV then developed a spear phishing email to send to Corporate Officer 1, purporting to originate from the Russian Federal Tax Service, in an attempt to gain unauthorized access to another non-Yahoo email account the officer controlled. The targeting of the Russian Financial Firm continued into 2016. Specifically, on or about January 13, 2016, the conspirators used Yahoo's AMT to access data associated with the account of the above-referenced board member's secretary.

37. BELAN also stole financial information from certain Yahoo user accounts for personal gain. For example, on or about April 26, 2015, BELAN searched within a victim user's account for credit card verification values ("cvv" numbers). As another example, on or about June 20, 2015, he did the same within a different user account, in addition to searching for "amex"; then he moved to another victim account and searched for, among other terms, "visa," "amex," "mastercard," and "credit . . . card"; then searched for those same terms in yet another user's account on the same day. In all, BELAN sought financial information from at least eight Yahoo users' accounts that day.

38. BELAN sought to steal gift card information from victim email accounts as well. For example, on or about October 8, 2016, BELAN searched the email accounts of at least 15 Yahoo victim users for gift cards, including by searching for the email address from which a major U.S. online retailer sent gift cards to its customers.

39. In addition, BELAN used his access to Yahoo's network to further a spam marketing scheme by minting cookies that enabled access to more than 30 million victim user accounts. From at least in or around March 2015 until in or around July 2015, BELAN used a malicious script he placed on Yahoo's network to mint cookies in bulk (up to at least tens of thousands of cookies at a time). Using computers under his control, including the BELAN Computer, BELAN minted in bulk cookies that were later used to steal the email contacts of the victim accounts; such contacts are valuable to spammers because they permit spammers to send emails purporting to originate from associates or acquaintances of targeted recipients, making it more likely the targeted recipient will open the spam email. Thousands of the bulk-minted cookies were removed from Yahoo's network to the BELAN Computer.

40. As they victimized Yahoo, the conspirators took steps to conceal their actions from Yahoo and law enforcement. For example, BELAN downloaded to Yahoo's network from the BELAN Computer a program known as a "log cleaner." This program sought to remove traces of the intrusion from Yahoo's records (logs) of network activity, to make the conspirators more difficult to track.

41. Finally, the conspirators used the stolen Yahoo data to compromise related user accounts at Yahoo, Google, and other webmail providers, including the Russian Webmail Provider. Among other means, they exploited the Yahoo data by searching within victim user accounts for other Yahoo or non-Yahoo accounts controlled by the same victim that the conspirators could later target for unauthorized

access; passwords; challenge question answers; and other information of use to the conspirators. For example:

a. On or about August 31, 2015, BELAN gained access to a Yahoo user account, then searched for terms including "password" and "Google" and phrases including "Google . . . account," "Apple . . . account," and "itunes . . . account."

b. On or about September 29, 2015, BELAN gained access to a Yahoo user account controlled by an officer of a U.S.-based technology and internet-related services company (the "U.S. Technology Company") and then searched that account for terms and phrases including "[U.S. Technology Company]" . . . password," "VPN," and "[Yahoo user name]@[U.S. Technology Company].com."

The Google and Other Account Intrusions

42. During the same period that DOKUCHAEV, SUSHCHIN, and BELAN were committing intrusions into the Yahoo computer network and the accounts of individual Yahoo users, DOKUCHAEV and SUSHCHIN were directing BARATOV to access individual accounts provided by Google, the Russian Webmail Provider, and other webmail providers. For example, the conspirators sought unauthorized access to the accounts of:

a. An assistant to the Deputy Chairman of the Russian Federation;

b. A managing director, a former sales officer, and a researcher, all of whom worked for a major Russian cyber security firm;

c. An officer of the Russian Ministry of Internal Affairs assigned to that Ministry's "Department K," its "Bureau of Special Technical Projects," which investigates cyber, high technology, and child pornography crimes;

d. A physical training expert working in the Ministry of Sports of a Russian republic; and

e. A Russian official who was both Chairman of a Russian Federation Council committee and a senior official at a major Russian transport corporation.

43. In some cases, DOKUCHAEV and SUSHCHIN identified target accounts based on information obtained through unauthorized access to Yahoo's network and its users' accounts. For example, on or about October 9, 2014, the conspirators accessed records for account

******as@yahoo.com in the AMT, associated with the CEO of a metals industry holding company in a country bordering Russia. Using the AMT, they changed the Yahoo user's recovery email account to an account controlled by DOKUCHAEV; then, approximately five minutes later, DOKUCHAEV falsely verified the change by clicking on an email link automatically generated by Yahoo. DOKUCHAEV then changed the account password. The next day, on or about October 10, 2014, DOKUCHAEV asked BARATOV to gain access to ******as@gmail.com, the account that had served as ******as@yahoo.com's recovery email account until DOKUCHAEV's change the day before.

44. Also on or about October 9, 2014, DOKUCHAEV sought unauthorized access to account ********ov@yahoo.com, belonging to a prominent banker and university trustee in a country bordering Russia. DOKUCHAEV changed the recovery account to one DOKUCHAEV controlled and changed the victim account password. Then, on or about October 10, 2014, DOKUCHAEV tasked BARATOV with gaining unauthorized access to ********ov@gmail.com, the account that had served as ********ov@yahoo.com's recovery email account until DOKUCHAEV's change the day before.

45. In other instances, the conspirators used their unauthorized access to Yahoo's network to obtain additional information about individuals who controlled accounts at other webmail providers to which the conspirators sought unauthorized access. For example,

a. On or about February 25, 2016, the conspirators gained unauthorized access to information in the AMT regarding a Yahoo account belonging to an International Monetary Fund official. One week later, on or about March 2, 2016, the conspirators gained access to that account by minting a cookie. That same day, the conspirators searched within that Yahoo user account for a particular Google account belonging to a managing director of a finance and banking company in a country bordering Russia. Then, on or about March 24, 2016, DOKUCHAEV tasked BARATOV with gaining unauthorized access to that Google account.

b. In another example, on or about March 2, 2016, the conspirators searched a Yahoo account belonging to an advisor to a senior official in a country bordering Russia, for "**********va@gmail.com," an email account belonging to a prominent business woman from that country. Then, on or about March 24, 2016, DOKUCHAEV tasked

BARATOV with gaining access to the same, searched-for Google account, **********va@gmail.com.

46. SUSHCHIN also identified accounts to target that were associated with the Russian Financial Firm. For example, in or around April 2015, SUSHCHIN sent DOKUCHAEV a list of email accounts associated with Russian Financial Firm personnel and family members to target, including Google accounts. During these April 2015 communications, SUSHCHIN identified a Russian Financial Firm employee to DOKUCHAEV as the "main target." Also during these April 2015 communications, SUSHCHIN forwarded to DOKUCHAEV an email sent by that "main target's" wife to a number of other Russian Financial Firm employees. SUSHCHIN added the cover note "this may be of some use." In another example, between in or about December 2015 and May 2016, SUSHCHIN directed DOKUCHAEV, who in turn directed BARATOV, to obtain unauthorized access to the Google and other accounts of Victims A and B and their family (discussed in paragraph 34.b above).

47. During the conspiracy DOKUCHAEV tasked BARATOV with obtaining unauthorized access to at least 80 identified email accounts, including at least 50 identified Google accounts.

48. BARATOV knowingly and with intent to defraud sought unauthorized access to Google and other accounts on behalf of DOKUCHAEV and SUSHCHIN through techniques such as spear phishing. He created and maintained multiple email accounts for the purpose of sending spear phishing emails to victims that he targeted at DOKUCHAEV and SUSHCHIN's behest.

49. When BARATOV successfully obtained unauthorized access to a victim's account, he notified DOKUCHAEV and provided evidence of that access. He then demanded payment—generally approximately U.S. $100—via online payment services.

50. Once DOKUCHAEV sent BARATOV a payment, BARATOV provided DOKUCHAEV with valid, illicitly obtained account credentials permitting DOKUCHAEV, SUSHCHIN, and others known and unknown to thereafter access the victim's account without further assistance from BARATOV.

All in violation of Title 18, United States Code, Section 1030(b).

COUNT TWO: 18 U.S.C. § 1831(a)(5) – Conspiracy to Engage in Economic Espionage

51. Paragraphs 1 through 11 and 14 through 50 of this Indictment are hereby re-alleged and incorporated by reference as if set forth in full herein.

52. In connection with the management and protection of its user accounts, Yahoo developed and maintained proprietary technology that constituted trade secrets as defined in Title 18, United States Code, Section 1839(3), including:

a. Yahoo's UDB and the data therein, including user data such as the names of Yahoo users, identified recovery email accounts and password challenge answers, and Yahoo-created and controlled data regarding its users' accounts;

b. Yahoo's AMT, its method and manner of functioning and capabilities, and the data it contained and provided; and

c. Yahoo's cookie minting source code.

53. From at least in or about January 2014, until December 1, 2016, in the Northern District of California and elsewhere, the defendants,

DMITRY DOKUCHAEV,
IGOR SUSHCHIN, and
ALEXSEY BELAN,

together with others known and unknown to the Grand Jury, knowingly combined, conspired, and agreed to:

a. Knowingly and without authorization steal, appropriate, take, and by fraud, artifice, and deception obtain trade secrets belonging to Yahoo;

b. Knowingly and without authorization copy, duplicate, alter, replicate, transmit, deliver, send, communicate, and convey trade secrets belonging to Yahoo; and

c. Knowingly receive, buy, and possess trade secrets belonging to Yahoo, knowing the same to have been stolen, appropriated, obtained, and converted without authorization;

intending and knowing that the offenses would benefit a foreign government, namely Russia, and a foreign instrumentality, namely the FSB, in violation of Title 18, United States Code, Section 1831(a)(1), (2), and (3).

54. In furtherance of the conspiracy and to effect its objects, DOKUCHAEV, SUSHCHIN, and BELAN committed the following acts:

a. In or about October 2014, DOKUCHAEV accessed records for user accounts in Yahoo's AMT.

b. On or about November 10, 2014, BELAN stole the Yahoo UDB by removing at least a portion of it to the BELAN Computer.

c. On or about December 12, 2014, DOKUCHAEV minted an unauthorized cookie.

d. On or about July 16, 2015, BELAN minted in bulk cookies permitting access to at least 17,000 Yahoo user accounts.

e. On or about July 20, 2015, DOKUCHAEV instructed SUSHCHIN how to use minted cookies to access Yahoo user accounts.

f. On or about December 21, 2015, DOKUCHAEV minted a cookie for a Yahoo user account and then sent the minted cookie to SUSHCHIN.

g. On or about January 13, 2016, the conspirators accessed Yahoo's AMT to obtain unauthorized access to data associated with a Yahoo user account.

h. On or about March 25, 2016, BELAN used a minted cookie to gain access to a Yahoo user's account.

i. On or about May 5, 2016, DOKUCHAEV sent a minted cookie for a Yahoo user's account to SUSHCHIN.

j. On or about May 10, 2016, SUSHCHIN sent DOKUCHAEV screen shots of victim accounts, including a Yahoo user's account, to which SUSHCHIN had gained unauthorized access.

k. On or about July 25, 2016, DOKUCHAEV sent BELAN information regarding FSB law enforcement and intelligence investigations, and FSB tactics, including its use of informants to target hackers whose difficult-to-trace computer intrusion infrastructure made other means of surveillance more difficult.

All in violation of Title 18, United States Code, Section 1831(a)(5).

COUNT THREE: 18 U.S.C. § 1832(a)(5) – Conspiracy to Commit Theft of Trade Secrets

55. Paragraphs 1 through 11, 14 through 50, 52, and 54 of this Indictment are hereby re-alleged and incorporated by reference as if set forth in full herein.

56. From at least in or about January 2014, until December 1, 2016, in the Northern District of California and elsewhere, the defendants,

DMITRY DOKUCHAEV,
IGOR SUSHCHIN, and
ALEXSEY BELAN,

together with others known and unknown to the Grand Jury, knowingly combined, conspired, and agreed to:

a. Knowingly and without authorization steal, appropriate, take, and by fraud, artifice, and deception obtain trade secrets belonging to Yahoo that were related to a product or service used in and intended to be used in interstate and foreign commerce;

b. Knowingly and without authorization copy, duplicate, alter, replicate, transmit, deliver, send, communicate, and convey trade secrets belonging to Yahoo that were related to a product or service used in and intended to be used in interstate and foreign commerce; and

c. Knowingly receive, buy, and possess trade secrets belonging to Yahoo that were related to a product or service used in and intended to be used in interstate and foreign commerce, knowing the same to have been stolen, appropriated, obtained, and converted without authorization;

intending to convert those trade secrets to the economic benefit of someone other than Yahoo, and intending and knowing that the offense would injure Yahoo, in violation of Title 18, United States Code, Section 1832(a)(1), (2), and (3).

57. In furtherance of the conspiracy and to effect its objects, conspirators committed the overt acts alleged in paragraph 54.

All in violation of Title 18, United States Code, Section 1832(a)(5).

COUNTS FOUR THROUGH SIX: 18 U.S.C. § 1831(a)(1) and (4) – Economic Espionage

58. Paragraphs 1 through 11, 14 through 50, 52, and 54 of this Indictment are hereby re-alleged and incorporated by reference as if set forth in full herein.

59. In or about the dates set forth below, in the Northern District of California and elsewhere, the defendants,

DMITRY DOKUCHAEV,
IGOR SUSHCHIN, and
ALEXSEY BELAN,

knowingly stole and without authorization appropriated, took, and concealed, and by fraud, artifice, and deception obtained a trade secret belonging to Yahoo, and attempted to do so, intending and knowing that the offense would benefit a foreign government, specifically Russia, and a foreign instrumentality, specifically the FSB.

COUNT	IN OR ABOUT	NATURE OF ECONOMIC ESPIONAGE
FOUR	November-December 2014	Theft of at least a portion of Yahoo's UDB
FIVE	October 2014-March 2016	Theft of information regarding the functioning of the Yahoo AMT
SIX	August 2015	Theft of Yahoo cookie minting source code

All in violation of Title 18, United States Code, Sections 1831(a)(1) and (4), and 2.

COUNT SEVEN THROUGH NINE: 18 U.S.C. § 1832(a)(1) – Theft of Trade Secrets

60. Paragraphs 1 through 11, 14 through 50, 52, and 54 of this Indictment are hereby re-alleged and incorporated by reference as if set forth in full herein.

61. In or about the dates set forth below, in the Northern District of California and elsewhere, the defendants,

DMITRY DOKUCHAEV
ALEXSEY BELAN, and
IGOR SUSHCHIN,

knowingly stole and without authorization appropriated, took, and concealed, and by fraud, artifice, and deception obtained, a trade secret belonging to Yahoo, and attempted to do so, which was related to a product or service used in and intended to be used in interstate and foreign commerce, intending to convert that trade secret to the economic benefit of someone other than Yahoo, and intending and

knowing that the offense would injure Yahoo.

COUNT	IN OR ABOUT	TRADE SECRET THEFT
SEVEN	November-December 2014	Theft of at least a portion of Yahoo's UDB
EIGHT	October 2014-March 2016	Theft of information regarding the functioning of the Yahoo AMT
NINE	August 2015	Theft of Yahoo cookie minting source code

All in violation of Title 18, United States Code, Sections 1832(a)(1) and 2.

COUNT TEN: 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud

62. Paragraphs 1 through 11, 14 through 50, and 54 of this Indictment are hereby re-alleged and incorporated by reference as if set forth in full herein.

63. From at least in or about January 2014, until December 1, 2016, in the Northern District of California and elsewhere, the defendants,

DMITRY DOKUCHAEV,
IGOR SUSHCHIN and
ALEXSEY BELAN,

together with others known and unknown to the Grand Jury, conspired to devise a scheme and artifice to defraud and to obtain property from Yahoo and Yahoo users by means of materially false and fraudulent pretenses, representations, and promises, and did knowingly transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, namely transmitting malicious computer code, illicitly obtained credentials, and fraudulent messages, for the purpose of executing and attempting to execute the scheme and artifice.

64. Specifically, DOKUCHAEV, SUSHCHIN, and BELAN conspired to devise a scheme whereby BELAN gained unauthorized access to Yahoo's network, among other means by stealing and employing Yahoo employee credentials. It was further part of the scheme that BELAN provided access to Yahoo's network to DOKUCHAEV and SUSHCHIN who, with BELAN, stole, created, and employed account credentials, including minted authentication cookies, to obtain unauthorized access to Yahoo data and user accounts.

65. DOKUCHAEV, SUSHCHIN, and BELAN thereby fraudulently obtained property from Yahoo and Yahoo users' accounts, including among other items, non-public information of value to each of the conspirators; gift card numbers redeemable at online merchants; access to payment accounts

such as PayPal and Western Union accounts; information about credit card cvv numbers; and the contacts of Yahoo users.

66. In furtherance of the scheme to defraud, BELAN also manipulated Yahoo search engine code for personal financial gain.

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

COUNTS ELEVEN THROUGH THIRTEEN: 18 U.S.C. § 1030(a)(2)(C) – Unauthorized Access to Protected Computers

67. Paragraphs 1 through 11, 14 through 50, and 54 of this Indictment are hereby re-alleged and incorporated by reference as if set forth in full herein.

68. On or about the dates set forth below, in the Northern District of California and elsewhere, the defendants

DMITRY DOKUCHAEV,
IGOR SUSHCHIN, and
ALEXSEY BELAN,

intentionally and without authorization attempted to access and did access a protected computer belonging to Yahoo, and thereby obtained information for commercial advantage and private financial gain; obtained information in furtherance of criminal and tortious acts in violation of the laws of California, including invasion of privacy; and obtained information valued in excess of $5,000.

COUNT	ON OR ABOUT	NATURE OF ACCESS
ELEVEN	September 2014	Accessing and scanning of Yahoo's corporate network from a Yahoo server and the theft of information regarding Yahoo's network architecture.
TWELVE	November 10, 2014	Accessing of Yahoo's corporate network and the theft of at least a portion of Yahoo's UDB.
THIRTEEN	December 12, 2014	Accessing of Yahoo's corporate network and theft of at least a portion of Yahoo's UDB.

All in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i)-(iii), and 2.

COUNTS FOURTEEN THROUGH SEVENTEEN: 18 U.S.C. § 1030(a)(5)(A) –Damaging Protected Computers

69. Paragraphs 1 through 11, 14 through 50, and 54 of this Indictment are hereby re-alleged and incorporated by reference as if set forth in full herein.

70. On or about the dates set forth below, in the Northern District of California and elsewhere, the defendants

DMITRY DOKUCHAEV
IGOR SUSHCHIN, and
ALEXSEY BELAN,

knowingly attempted to cause 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 at least ten protected computers during a one-year period and causing more than $5,000 in loss in one year.

COUNT	ON OR ABOUT	DAMAGING ACT
FOURTEEN	October 30, 2014	Placement of malicious code on Yahoo's network to provide a means of facilitating the conspirators' future access to Yahoo's servers
FIFTEEN	November 10, 2014	Modification of code on Yahoo's system to direct certain Yahoo search engine users to an online pharmacy
SIXTEEN	June 8, 2015 through July 16, 2015	Placement of a malicious script onto Yahoo's network to internally mint cookies. The results of this script (cookies that would allow access to victims' accounts) were then exfiltrated
SEVENTEEN	August 13, 2015	Placement of a new script used to internally mint cookies onto Yahoo's network

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B), and 2.

COUNTS EIGHTEEN THROUGH TWENTY-FOUR: 18 U.S.C. § 1030(a)(2)(C) – Unauthorized Access to Protected Computers

71. Paragraphs 1 through 11, 14 through 50, and 54 of this Indictment are hereby re-alleged and incorporated by reference as if set forth in full herein.

72. On or about the dates set forth below, in the Northern District of California and elsewhere, the defendants

DMITRY DOKUCHAEV,
IGOR SUSHCHIN, and
ALEXSEY BELAN,

intentionally and without authorization attempted to access and did access a protected computer belonging to Yahoo, and thereby obtained and attempted to obtain information for commercial advantage and private financial gain; information in furtherance of criminal and tortious acts in violation of the laws of California, including invasion of privacy; and information valued in excess of $5,000.

COUNT	ON OR ABOUT	NATURE OF ACCESS
EIGHTEEN	April 16, 2016	BELAN accessed **********35@yahoo.com using a fraudulently minted cookie.
NINETEEN	February 26, 2016	DOKUCHAEV accessed ****ey@yahoo.com using a fraudulently minted cookie.
TWENTY	March 30, 2016	DOKUCHAEV accessed ****re4@yahoo.com using a fraudulently minted cookie.
TWENTY-ONE	May 17, 2016	BELAN accessed ********tter@yahoo.com using a fraudulently minted cookie.
TWENTY-TWO	May 18, 2016	BELAN accessed **********35@yahoo.com using a fraudulently minted cookie.
TWENTY-THREE	March 30, 2016	DOKUCHAEV accessed ********feld@yahoo.com using a fraudulently minted cookie.
TWENTY-FOUR	March 30, 2016	DOKUCHAEV accessed **********rosa@yahoo.com using a fraudulently minted cookie.

All in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i)-(iii), and 2.

COUNTS TWENTY-FIVE THROUGH THIRTY-SIX: 18 U.S.C. § 1029(a)(1) – Counterfeit Access Devices

73. Paragraphs 1 through 11, 14 through 50, and 54 of this Indictment are hereby re-alleged and incorporated by reference as if set forth in full herein.

74. On or about the dates set forth below, in the Northern District of California and elsewhere, the defendants,

DMITRY DOKUCHAEV,
IGOR SUSHCHIN, and
ALEXSEY BELAN,

did knowingly and with intent to defraud, produce, use, and traffic in at least one counterfeit access device, and attempted to do so.

COUNT	ON OR ABOUT	COUNTERFEIT ACCESS DEVICE
TWENTY-FIVE	July 16, 2015	BELAN minted at least 17,000 cookies.
TWENTY-SIX	July 20, 2015	DOKUCHAEV sent SUSHCHIN a minted cookie for ***tech@yahoo.com.
TWENTY-SEVEN	September 9, 2015	DOKUCHAEV produced and used a minted cookie to gain unauthorized access to account *******30@yahoo.com.
TWENTY-EIGHT	September 29, 2015	BELAN produced and used a minted cookie to gain unauthorized access to account **********on@yahoo.com.
TWENTY-NINE	September 29, 2015	BELAN produced and used a minted cookie to gain unauthorized access to account ******54@yahoo.com.
THIRTY	September 29, 2015	BELAN produced and used a minted cookie to gain unauthorized access to account ******on@yahoo.com.
THIRTY-ONE	September 29, 2015	BELAN produced and used a minted cookie to gain unauthorized access to account *********ey@yahoo.com.
THIRTY-TWO	September 29, 2015	BELAN produced and used a minted cookie to gain unauthorized access to account ********20@yahoo.com.
THIRTY-THREE	December 21, 2015	DOKUCHAEV sent SUSHCHIN a minted cookie for ******08@yahoo.com.
THIRTY-FOUR	April 25, 2016	DOKUCHAEV produced and used a minted cookie to gain unauthorized access to account *****ru@yahoo.com.
THIRTY-FIVE	April 25, 2016	DOKUCHAEV produced and used a minted cookie to gain unauthorized access to account **********ov@yahoo.com.
THIRTY-SIX	May 5, 2016	DOKUCHAEV sent SUSHCHIN a minted cookie for ******08@yahoo.com.

All in violation of Title 18, United States Code, Sections 1029(a)(1), 1029(b)(1), and 2.

COUNT THIRTY-SEVEN: 18 U.S.C. § 1029(a)(4) – Device Making Equipment

75. Paragraphs 1 through 11, 14 through 50, and 54, of this Indictment are hereby re-alleged and incorporated by reference as if set forth in full herein.

76. From in or about December 2015 until in or about March 2016, in the Northern District of California and elsewhere, the defendants,

DMITRY DOKUCHAEV,
IGOR SUSHCHIN, and
ALEXSEY BELAN,

did knowingly and with intent to defraud produce, traffic in, have control and custody of, and possess device-making equipment, and attempted to do so, to wit, tools and software that could be and were used to mint unauthorized cookies permitting unauthorized access to Yahoo user accounts, as alleged in paragraph 74.

All in violation of Title 18, United States Code, Sections 1029(a)(4) and 2.

COUNT THIRTY-EIGHT: 18 U.S.C. § 1029(b)(2) – Conspiracy to Commit Fraud in Connection with Access Devices

77. Paragraphs 1 through 11, 14 through 50, and 54, and the factual allegations set forth in paragraph 75 of this Indictment are hereby re-alleged and incorporated by reference as if set forth in full herein.

78. From at least in or about January 2014, until December 1, 2016, in the Northern District of California and elsewhere, the defendants,

DMITRY DOKUCHAEV,
IGOR SUSHCHIN, and
KARIM BARATOV,

and others known and unknown, knowingly conspired, combined, and agreed to, and did, with intent to defraud, in an offense affecting interstate and foreign commerce:

a. traffic in and use at least one unauthorized access device during a one-year period, to obtain something of value aggregating at least $1,000 during that period, in violation of Title 18, United States Code, Section 1029(a)(2); and

b. effect transactions, with at least one access device issued to another person, to receive payment and another thing of value during a one-year period, the aggregate value of which was at least $1,000, in violation of Title 18, United States Code, Section 1029(a)(5).

79. Specifically, BARATOV sought and gained unauthorized access to Google and other webmail provider accounts as requested by DOKUCHAEV, sometimes after DOKUCHAEV's discussions with SUSHCHIN. BARATOV provided the means of unauthorized access in the form of valid, but illicitly obtained passwords, to DOKUCHAEV. DOKUCHAEV then paid BARATOV for providing DOKUCHAEV with such information, thereby enabling unauthorized access to the requested

email accounts. In total, DOKUCHAEV paid BARATOV money and other things of value aggregating at least $1,000 for unauthorized email account access during a one-year period, from April 17, 2015 through April 17, 2016.

OVERT ACTS

80. In furtherance of the conspiracy and to effect its illegal objects, BARATOV, DOKUCHAEV, and SUSHCHIN committed the following acts:

a. On or about October 10, 2014, DOKUCHAEV sent BARATOV a request for unauthorized access to ******as@gmail.com and ********ov@gmail.com.

b. On or about October 10, 2014, DOKUCHAEV sent BARATOV a request for unauthorized access to more than 30 Google accounts, not including the two described in the preceding paragraph.

c. On or about December 26, 2014, BARATOV sent DOKUCHAEV the password for *******17@gmail.com, to which account DOKUCHAEV had tasked BARATOV to gain unauthorized access.

d. On or about January 2, 2015, BARATOV sent DOKUCHAEV the password for *****2011@gmail.com, to which account DOKUCHAEV had tasked BARATOV to gain unauthorized access.

e. On or about July 6, 2015, BARATOV sent DOKUCHAEV the password for *****77@gmail.com, to which account DOKUCHAEV had tasked BARATOV to gain unauthorized access.

f. On or about August 1, 2015, BARATOV sent DOKUCHAEV a second password for *****2011@gmail.com, an account for which BARATOV had sent DOKUCHAEV a password on or about January 2, 2015, and, to which account DOKUCHAEV had tasked BARATOV to gain unauthorized access

g. On or about September 30, 2015, BARATOV sent DOKUCHAEV the password for *******um@gmail.com, to which account DOKUCHAEV had tasked BARATOV to gain unauthorized access.

h. On or about November 16, 2015, DOKUCHAEV sent BARATOV a request for unauthorized access to ****br@gmail.com and ****ov@gmail.com.

i. On or about November 17, 2015, BARATOV sent DOKUCHAEV the password for ****ov@gmail.com, to which account DOKUCHAEV had tasked BARATOV to gain unauthorized access.

j. On or about November 17, 2015, DOKUCHAEV paid BARATOV U.S. $104.20.

k. On or about December 3, 2015, BARATOV sent DOKUCHAEV the password for ********13@gmail.com, to which account DOKUCHAEV had tasked BARATOV to gain unauthorized access.

l. On or about March 24, 2016, DOKUCHAEV sent BARATOV a request for unauthorized access to **********va@gmail.com.

m. On or about March 25, 2016, BARATOV sent DOKUCHAEV the password for ********21@gmail.com, to which account DOKUCHAEV had tasked BARATOV to gain unauthorized access.

All in violation of Title 18, United States Code, Sections 1029(b)(2).

COUNT THIRTY-NINE: 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud

81. Paragraphs 1 through 11, 14 through 50, 54, and 80, and the factual allegations set forth in paragraph 74 of this Indictment are hereby re-alleged and incorporated by reference as if set forth in full herein.

82. From at least in or about January 2014, until December 1, 2016, in the Northern District of California and elsewhere, the defendants,

DMITRY DOKUCHAEV,
IGOR SUSHCHIN and
KARIM BARATOV,

together with others known and unknown to the Grand Jury, conspired to devise a scheme and artifice to defraud and to obtain property from Google account users by means of materially false and fraudulent pretenses, representations, and promises, and did knowingly transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures, and

sounds, namely transmitting malicious computer code, illicitly obtained credentials, and fraudulent messages, for the purpose of executing and attempting to execute the scheme and artifice, in violation of Title 18, United States Code, Section 1343.

83. Specifically, DOKUCHAEV and SUSHCHIN identified email accounts to which they wanted access. DOKUCHAEV then directed BARATOV to attempt to gain unauthorized access to at least 80 email accounts, including at least 50 Google accounts. BARATOV attempted to obtain access credentials for the accounts through "spear phishing." BARATOV, when successful, sent DOKUCHAEV the passwords for the accounts.

84. Upon successfully gaining the credentials for a tasked account, BARATOV informed DOKUCHAEV that he could be paid for his work in Russian rubles, U.S. dollars, Ukrainian hryvnia, or Euros through online payment services. DOKUCHAEV then paid BARATOV using these means.

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

COUNTS FORTY THROUGH FORTY-SEVEN: 18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft

85. Paragraphs 1 through 50 and 80 of this Indictment are hereby re-alleged and incorporated by reference as if set forth in full herein.

86. On or about the dates set forth below, in the Northern District of California and elsewhere, the defendants,

DMITRY DOKUCHAEV and
KARIM BARATOV,

during and in relation to the crimes of Conspiracy to Commit Computer Fraud, in violation of 18 U.S.C. Section 1030(b), Unauthorized Access to Computers, in violation of 18 U.S.C. Section 1030(a)(2), Conspiracy to Commit Fraud and Related Activity in Connection with Access Devices, in violation of 18 U.S.C. Section 1029(b)(2), and Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. Section 1349, did knowingly transfer, possess, and use, without lawful authority, the means of identification of another person.

COUNT	ON OR ABOUT	IDENTIFICATION OF ANOTHER PERSON
FORTY	December 26, 2014	BARATOV sent DOKUCHAEV the password and email address for *******17@gmail.com.
FORTY-ONE	January 2, 2015	BARATOV sent DOKUCHAEV the password and email

		address for *****2011@gmail.com.
FORTY-TWO	July 6, 2015	BARATOV sent DOKUCHAEV the password and email address for *****77@gmail.com.
FORTY-THREE	August 1, 2015	BARATOV sent DOKUCHAEV the password and email address for *****2011@gmail.com.
FORTY-FOUR	September 30, 2015	BARATOV sent DOKUCHAEV the password and email address for *******um@gmail.com.
FORTY-FIVE	November 17, 2015	BARATOV sent DOKUCHAEV the password and email address for ****ov@gmail.com.
FORTY-SIX	December 3, 2015	BARATOV sent DOKUCHAEV the password and email address for ********13@gmail.com.
FORTY-SEVEN	March 25, 2016	BARATOV sent DOKUCHAEV the password and email address for ********21@gmail.com.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2, and Title 28, United States Code, Section 3238.

FIRST FORFEITURE ALLEGATION: 18 U.S.C. § § 982(a)(2)(B) & 1030(i) and (j)

87. The allegations contained in paragraphs one to eleven and Counts One and Eleven through Twenty-Four are hereby re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i) and (j).

88. Upon conviction of any of the offenses in violation of Title 18, United States Code, Section 1030 as set forth in Counts One and Eleven through Twenty-Four of this Indictment, defendants

DMITRY DOKUCHAEV,
ALEXSEY BELAN,
IGOR SUSHCHIN, and
KARIM BARATOV,

shall forfeit to the United States of America:

a. pursuant to Title 18, United States Code, Sections 982(a)(2)(B), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of said violations; and

b. pursuant to Title 18, United States Code, Sections 1030(i) and (j), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of said violations, and any property used to commit or facilitate the commission of said violation or conspiracy thereto.

89. The property subject to forfeiture shall include, but not be limited to the following:

a. All funds which constitute proceeds that are held on deposit in PayPal account number xxxxxxxxxxxxxxx9844, held by BARATOV in the name of "Elite Space Corporation";

b. All funds which constitute proceeds that are held on deposit in PayPal account number xxxxxxxxxxxxxxx2639, held by DOKUCHAEV;

c. a grey Aston Martin DBS, license plate identification "MR KARIM"; and

d. a black Mercedes Benz C54, license plate identification "CAWE693."

90. If, as a result of any act or omission of the defendants, any of said property:

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

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

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 without difficulty cannot be subdivided;

any and all interest defendants have in any other property (not to exceed the value of the above forfeitable property), including but not limited to a grey Aston Martin DBS, license plate identification "MR KARIM," and a black Mercedes Benz C54, license plate identification "CAWE693," shall be forfeited to the United States, pursuant to Title 21, United States Code, Section 853(p) and as incorporated in Title 28, United States Code, Sections 2323(b).

SECOND FORFEITURE ALLEGATION: 18 U.S.C. § § 1834 and 2323

91. The allegations contained in paragraphs one to eleven and Counts Two through Nine are hereby re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 1834 and 2323.

92. Upon conviction of any of the offenses in violation of Title 18, Unite States Code, Section 1030 as set forth in Counts Two through Nine of this Indictment, defendants

DMITRY DOKUCHAEV,
ALEXSEY BELAN, and
IGOR SUSHCHIN,

shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections 1834 and 2323, any property used or intended to be used in any manner or part to commit or facilitate the

offenses, and any property constituting or derived from the proceeds obtained directly or indirectly as a result of said offenses.

93. The property subject to forfeiture shall include, but not be limited to all funds which constitute proceeds that are held on deposit in PayPal account number xxxxxxxxxxxxxxx2639, held by DOKUCHAEV.

94. If, as a result of any act or omission of the defendants, any of said property:

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

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

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 without difficulty cannot be subdivided;

any and all interest defendants have in any other property (not to exceed the value of the above forfeitable property), including but not limited to a grey Aston Martin DBS, license plate identification "MR KARIM," and a black Mercedes Benz C54, license plate identification "CAWE693," shall be forfeited to the United States, pursuant to Title 21, United States Code, Section 853(p) and as incorporated in Title 28, United States Code, Sections 2323(b).

THIRD FORFEITURE ALLEGATION: 18 U.S.C. § §981(a)(1)(C), 982(a)(2)(B) and 1029(c)(1)(C) and 28 U.S.C. § 2461(c)

95. The allegations contained in paragraphs one to eleven and Counts Ten and Twenty-Five through Thirty-Eight are hereby re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections (a)(2)(B) and 1029(c)(1)(C) and Title 28, United States Code, Section 2461(c).

96. Upon conviction of any of the offenses in violation of Title 18, United States Code, Sections 1029 and 1349 as set forth in Counts Ten and Twenty-Five through Thirty-Eight of this Indictment, defendants

DMITRY DOKUCHAEV,
ALEXSEY BELAN,
IGOR SUSHCHIN, and
KARIM BARATOV,

shall forfeit to the United States of America:

a. pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to these violations;

b. pursuant to Title 18, United States Code, Section 982(a)(2)(B), any property constituting or derived from proceeds obtained directly or indirectly as a result of these violations;

c. pursuant to Title 18, United States Code, Section 1029(c)(1)(C), any personal property used or intended to be used to commit a violation of Title 18, United States Code, Section 1029.

97. The property subject to forfeiture shall include, but not be limited to the following:

a. All funds which constitute proceeds that are held on deposit in PayPal account number xxxxxxxxxxxxxxx9844 held by BARATOV in the name of" Elite Space Corporation";

b. All funds which constitute proceeds that are held on deposit in PayPal account number xxxxxxxxxxxxxxx2639, held by DOKUCHAEV;

c. a grey Aston Martin DBS, license plate identification "MR KARIM"; and

d. a black Mercedes Benz C54, license plate identification "CAWE693."

98. If, as a result of any act or omission of the defendants, any of said property:

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

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

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 without difficulty cannot be subdivided;

any and all interest defendants have in any other property (not to exceed the value of the above forfeitable property), including but not limited to a grey Aston Martin DBS, license plate identification

"MR KARIM," and a black Mercedes Benz C54, license plate identification "CAWE693," shall be forfeited to the United States, pursuant to Title 21, United States Code, Section 853(p) and as incorporated in Title 28, United States Code, Sections 2461(c).

DATED: 2/28/17

A TRUE BILL

[redacted]

FOREPERSON

BRIAN J. STRETCH
United States Attorney

BARBARA J. VALLIERE
Chief, Criminal Division

(Approved as to form: _____)
AUSA John Hemann
NSD Trial Attorney Scott McCulloch
NSD Cyber Counsel Christopher Ott

Exhibit A

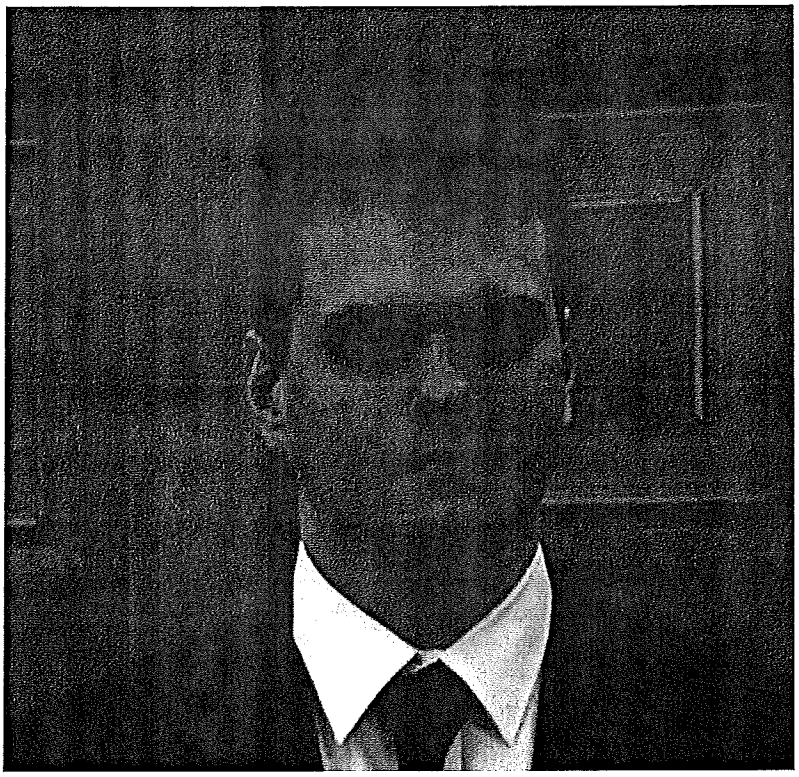

Exhibit B

Exhibit C

Exhibit D