IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. MIKHAIL TSAREV, aka MANGO, ANDREY ZHUYKOV, aka ZHUIKOV, aka DIF, aka DEF, aka DEFENDER, MAKSIM GALOCHKIN, aka BENTLEY, DMITRY PUTILIN, aka GRAD, aka STAFF, SERGEY LOGUNTSOV, aka BEGEMOT, aka ZULAS, MAX MIKHAYLOV, aka BAGET, MAKSIM RUDENSKY, aka FONIN, aka BINMAN, VALENTIN KARYAGIN, aka GLOBUS, MAKSIM KHALIULLIN, aka MAXFAX, aka MAXHAX, aka KAGAS, Defendants.	)	INDICTMENT CASE NO. 1:23 CR 00309 Title 18, United States Code, Sections 371, 1349, 1956(h), 3559(g)(1) and 2 **JUDGE FLEMING**

GENERAL ALLEGATIONS

At all times relevant to this Indictment:

1. Defendants MIKHAIL TSAREV, aka MANGO; ANDREY ZHUYKOV, aka ZHUIKOV, aka DIF, aka DEF, aka DEFENDER; MAKSIM GALOCHKIN, aka BENTLEY;

DMITRY PUTILIN, aka GRAD, aka STAFF; SERGEY LOGUNTSOV, aka BEGEMOT, aka ZULAS; MAX MIKHAYLOV, aka BAGET; MAKSIM RUDENSKY, aka FONIN, aka BINMAN; VALENTIN KARYAGIN, aka GLOBUS; and MAKSIM KHALIULLIN, aka MAXFAX, aka MAXHAX, aka KAGAS and others known and unknown to the Grand Jury (hereinafter referred to as the "Trickbot Group") were participants in a criminal scheme to defraud and were located in or around Russia, Belarus, Ukraine, and elsewhere.

DEFINITIONS

2. "Malware" was malicious or intrusive software designed to disrupt computer operations, gather sensitive information, gain access to private computer systems, or commit other unauthorized actions on a computer system. Malware was installed on a computer without the knowledge or permission of the owner. Common examples of malware included viruses, worms, trojans, keyloggers, and spyware.

3. A "trojan" was a type of malware which masqueraded as a routine download request or as an opportunity to download files of interest to the user in order to persuade the victim to install it. Many trojans, including the Trickbot Trojan[1] discussed below, acted as an unauthorized access point to the victim computer that allowed an unauthorized computer to access and communicate with the infected computer.

4. "Keystroke logging" was the action of recording or logging the keys struck on a keyboard. This action usually was done surreptitiously by a computer program, such as a keylogger, to capture the keys typed on a computer without the typist's knowledge. Malware

---

[1] For purposes of this Indictment, the terms "Trickbot," "Trickbot malware," and "Trickbot Trojan" are used interchangeably, and all refer to the same suite of malware tools used by Defendants and other Trickbot Conspirators.

that used keystroke logging often would provide the captured keystrokes to the individual who caused the malware to be installed or to a place designated by that individual. Through keystroke logging, individuals were able to obtain online banking credentials as soon as the user of the infected computer logged into their account. After obtaining this information, these individuals could then access the victim's online bank account and execute unauthorized electronic funds transfers, such as Automated Clearing House (ACH) payments or wire transfers,[2] to accounts that they controlled.

5. "Hypertext Transfer Protocol" (HTTP) was the protocol used to transfer data over the internet. The primary function of HTTP was to establish a connection between computers and servers on the internet to transfer information, including web pages and downloadable files, from internet-connected servers to computers using internet browsers.

6. "HTTP GET" was a command in HTTP that allowed a user to request information from a web server. An example of an HTTP GET command would be to enter a bank URL in the address bar of an internet browser, which would then send a request for information about the bank web page to the corresponding web server.

7. "HTTP POST" was a command in HTTP that allowed the user to interact with and update information on a web server. An example of an HTTP POST command would be

---

[2] Electronic funds transfers were the exchange and transfer of money through computer-based systems using the internet. ACH payments allowed the electronic transferring of funds from one bank account to another bank account within the ACH network without any paper money changing hands. The ACH network was a network of participating depository financial institutions across the United States, and the network provided for interbank clearing of electronic payments. Because ACH payments required the network to clear the transaction, the funds were not immediately available. Wire transfers also allowed electronic transferring of funds from one bank account to another bank account without any paper money changing hands; however, unlike ACH payments, wire transferred funds were immediately available.

when a user who was already on a bank web page entered information on that page, such as their online credentials, and thus interacted with the web server itself.

8. "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. Different injects were used for different purposes. Some 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 individual employing the web inject. Web injects often interacted with HTTP GET and HTTP POST commands.

9. A "bot" was a computer infected with malware without the knowledge of the computer's user and controlled remotely by another individual. For purposes of this Indictment, all "bots" were infected computers and all infected computers were bots. A "botnet" was an interconnected network of bots.

10. A "command and control server" was a centralized computer that issued commands to the bots in a botnet and received reports back from the bots. A "Command and Control" (C2) infrastructure consisted of servers and other technical infrastructure used to control malware in general and, in particular, botnets. C2 servers either could be controlled directly by the malware operators or run on hardware compromised by malware.

11. A "virtual private network" (VPN) was a technology that created a secure network connection over a public network such as the internet or a private network owned by an Internet Service Provider. By using a VPN, a user could conceal his or her true IP address from those with whom he or she was communicating.

12. A "virtual private server" (VPS) was a virtual machine sold as a service by an Internet Service Provider.

13. A "loader" was a basic remote access trojan. A loader is designed to install additional malware components onto a victim computer and to evade detection by anti-virus programs.

14. A "worm" described the process of malware moving laterally within a network, replicating itself from an initial infected computer to other computers on a network to diversify a malware's footprint on an infected network.

15. "Multi-Factor Authentication" was a common security feature used by web-based services, such as banks, that stored confidential personal and online financial information. Multi-Factor Authentication required the use of multiple independent mechanisms to verify the authenticity and identity of the user. Examples of Multi-Factor Authentication included the concurrent use of a password known by a user and an authentication token, such as a SMS code sent to the user's telephone.

16. "Ransomware" was a type of malware designed to deny a victim access to his or her computer and/or computer files until the payment of a ransom. Ransomware could also be used to steal data and threaten its release unless a ransom is paid.

17. A "Mule" or "Money Mule" was a person who received stolen funds into his or her bank account and then moved the money to other accounts, often overseas.

18. A "Cryptocurrency Mixer" was a service used by individuals to conceal the source of cryptocurrency. This was done by disassociating incoming bitcoin from particular bitcoin addresses or transactions and then comingling that bitcoin with other incoming bitcoin prior to conducting any exchange. This process allowed users engaged in unlawful activities to launder their proceeds by concealing the nature, source, location and destination of their "dirty" cryptocurrency.

19. A "Malware Manager" was a member of the scheme generally responsible for recruiting and hiring "Malware Developers" (defined below), procuring infrastructure, managing finances, testing malware against Counter Anti-Virus services (defined below), and deploying and monitoring the malware.

20. A "Malware Developer" was a member of the scheme generally responsible for writing the software code for the malware and updating it over time. Malware Developers would also set up the "backend infrastructure" of the malware, including setting up and updating the servers procured by malware managers.

21. "Phishing" was a criminal scheme in which the perpetrators used mass email messages and/or fake websites to trick a victim into providing information, such as network credentials (e.g., usernames and passwords), that could later be used to gain access to the victim's systems. Phishing schemes often used social engineering techniques similar to traditional con-artist techniques in order to trick a victim into believing he or she was providing his or her information to a trusted vendor, customer, or other acquaintance. Phishing emails were also used to trick a victim into clicking on documents or links that contained malicious software that then infected and compromised the victim's computer system without his or her knowledge or permission.

22. "Spear phishing" was a targeted form of phishing directed towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals also used spear phishing schemes to install malware on a targeted user's computer.

23. "Crypting" was the process of encrypting malware to avoid detection by anti-virus tools and software on victims' computers.

24. "Crypted" malware was subjected to crypting.

25. A "GitLab" was an online software development platform used for storing, tracking, and collaborating on software projects. It enables programmers to upload their own code files and collaborate with others.

26. "Counter Anti-Virus" services checked malware against anti-virus software to determine if the malware would be detected by the anti-virus software. Counter Anti-Virus services did not share and distribute uploaded malware files with anti-virus companies, but instead provided anonymity to Malware Developers and users.

27. Unsolicited "SPAM" consisted of commercial electronic mail messages sent in bulk to recipients without prior request or approval. Individuals responsible for sending or causing the distribution of SPAM were referred to as spammers.

28. A "backdoor" was a program used to access a computer discretely while bypassing the authentication and security requirements. Backdoors allow for remote control and code execution on a computer system or network.

INDIVIDUALS AND ENTITIES

29. The following were financial institutions, within the meaning of Title 18, United States Code, Section 20, whose deposits were insured by the Federal Deposit Insurance Corporation (collectively, the "Financial Institutions"):

a. Buckeye Community Bank;

b. First National Bank;

c. Huntington National Bank;

d. J.P. Morgan Chase Bank;

e. Key Bank;

f. People's United Bank;

g. Regions Bank; and

h. U.S. Bank.

30. CoBank was a financial institution within the meaning of Title 18, United States Code, Section 20, and was a system institution of the Farm Credit System, as defined in Section 5.35(3) of the Farm Credit Act of 1971.

31. Cooperating Witness 1 (CW 1) was a public school district located in Avon, Ohio, in the Northern District of Ohio, Eastern Division.

32. Cooperating Witness 2 (CW 2) was a public school district located in Akron, Ohio, in the Northern District of Ohio, Eastern Division.

33. Cooperating Witness 3 (CW 3) was a real estate firm located in North Canton, Ohio, in the Northern District of Ohio, Eastern Division.

34. Cooperating Witness 4 (CW 4) was a country club located in Ripon, California.

35. Cooperating Witness 5 (CW 5) was a law firm located in Ft. Myers, Florida.

36. Cooperating Witness 6 (CW 6) was a school district located in Bennington, Vermont.

37. Cooperating Witness 7 (CW 7) was a country club located in Lynchburg, Virginia.

38. Cooperating Witness 8 (CW 8) was an electrical service company located in Eastland, Texas.

39. Cooperating Witness 9 (CW 9) was a county government located in Tulare, California.

40. Cooperating Witness 10 (CW 10) was a staffing services company located in New York, New York.

41. Cooperating Witness 11 (CW 11) was an agricultural company located in Minnesota.

42. Unless otherwise noted, all communications of Defendants and other Trickbot Conspirators set forth in this Indictment were translated from Russian to English.

THE TRICKBOT SCHEME TO DEFRAUD

43. "Dyre" was an online banking trojan operated by individuals known and unknown to the Grand Jury based in Moscow, Russia, and began targeting non-Russian businesses and entities in mid-2014. In or around November 2015, Russian authorities arrested numerous individuals at 25th Floor, a Moscow-based film company associated with Dyre. Although Dyre activity slowed significantly after the purported Russian action, no charges against members of the Dyre network or 25th Floor were made public. In the months and years following the Russian authorities' purported actions, the Dyre actors regrouped and created a new suite of malware tools known as Trickbot.

44. From in or around November 2015 and continuing through the date of this Indictment, Defendants MIKHAIL TSAREV, aka MANGO; ANDREY ZHUYKOV, aka ZHUIKOV, aka DIF, aka DEF, aka DEFENDER; MAKSIM GALOCHKIN, aka BENTLEY; DMITRY PUTILIN, aka GRAD, aka STAFF; SERGEY LOGUNTSOV, aka BEGEMOT, aka ZULAS; MAX MIKHAYLOV, aka BAGET; MAKSIM RUDENSKY, aka FONIN, aka BINMAN; VALENTIN KARYAGIN, aka GLOBUS; and MAKSIM KHALIULLIN, aka MAXFAX, aka MAXHAX, aka KAGAS, and others known and unknown to the Grand Jury, were part of a transnational organized cybercrime network that stole money and personal and confidential information from unsuspecting victims, including businesses and their financial

institutions located in the United States, United Kingdom, Australia, Belgium, Canada, Germany, India, Italy, Japan, Mexico, Spain, and Russia, through the use of the Trickbot malware.

45. Specifically, Defendants and other members of the scheme (collectively hereinafter the "Trickbot Conspirators" or "Trickbot Group") worked to: (a) infect victims' computers with Trickbot malware designed to capture victims' online banking login credentials; (b) obtain and harvest other personal identification information, including credit cards, emails, passwords, dates of birth, social security numbers, and addresses; (c) infect other computers connected to the victim computer; (d) use the captured login credentials to fraudulently gain unauthorized access to victims' online bank accounts at financial institutions; (e) steal funds from victims' bank accounts and launder those funds using U.S. and foreign beneficiary bank accounts provided and controlled by Defendants and other Trickbot Conspirators; and (f) facilitate the installation of ransomware on victim computers.

46. Members of the scheme (Trickbot Conspirators) were located in multiple countries around the world including, but not limited to, Russia, Belarus, Ukraine, and elsewhere.

47. To perpetrate their criminal schemes, Defendants used a network of associates who provided specialized services and technical abilities in furtherance of the criminal scheme. The specialized skills and services included soliciting and recruiting malware developers; purchasing and managing servers from which to test, deploy, and operate the Trickbot malware; encrypting the malware to avoid detection by anti-virus software; engaging in spamming, phishing and spear-phishing campaigns against potential victims; and coordinating the receipt and laundering of funds from the victims to Defendants and others.

48. Defendants created Trickbot to further their criminal scheme. Trickbot was a modular, multi-function suite of malware tools designed in part to automate the theft of confidential personal and financial information, such as online banking credentials, from infected computers through the use of web injects and keystroke logging. Later versions of Trickbot were adapted to facilitate the installation and use of ransomware.

49. Defendants used the framework and code from Dyre to establish the basis for the Trickbot malware, and used their connections to Dyre and to others involved in the development and use of Dyre to create Trickbot.

50. Trickbot was designed to evade detection by anti-virus software and other protective measures employed by victims and was generally spread through phishing and spear phishing campaigns.

51. Trickbot infected millions of victim computers worldwide.

52. In the United States, Trickbot primarily targeted victim computers belonging to U.S. businesses, entities and individuals, including those within the Northern District of Ohio.

53. Trickbot was used to attack critical infrastructure including hospitals, schools, financial institutions, and governments.

54. Once installed on a victim computer, Trickbot, in part, used web injects and keystroke logging to obtain and harvest online banking credentials from infected victim computers. Defendants then used these credentials to gain unauthorized access to victims' bank accounts and then transfer and attempt to transfer funds from the victims' accounts to accounts controlled by Defendants.

55. In or around Fall 2016, Trickbot began victimizing businesses, hospitals, schools, financial institutions, and individuals in the United States and worldwide.

56. In or around March 2020, Trickbot developers started to create their own ransomware. During development, the ransomware was named Locker or Cryptolocker. It was initially named Enigma and later Diavol.

57. The Diavol ransomware was used to infect victim computers starting in July 2021.

DEFENDANTS

58. Defendant MIKHAIL TSAREV (TSAREV), aka MANGO, was a citizen and national of Russia. During the timeframe of this Indictment, TSAREV was a manager and accountant for the Trickbot Group. As an accountant, TSAREV had the duty to pay salaries to members of the Trickbot Group from cryptocurrency wallets controlled by the Trickbot Group to individual Trickbot Conspirators' wallets. Using the monikers "Khano," "dirty_f***er_fritzzz," and "bomba777," among others known to the Grand Jury, TSAREV discussed Trickbot structure, salaries, and finances with other managers of the Trickbot Group.

59. Defendant ANDREY ZHUYKOV (ZHUYKOV), aka ZHUIKOV, aka DIF, aka DEF, aka DEFENDER, was a citizen and national of Russia. During the timeframe of this Indictment, ZHUYKOV resided in Sochi, Russia and used the online monikers "dif," "def," and "defender." ZHUYKOV was a malware developer and computer programmer for Trickbot, responsible for managing developers' access to the group's servers, configuring Jabber and development servers for use by the Trickbot Group, and creating automated processes for using stolen personal identification information to purchase goods. ZHUYKOV provided completed modules of Trickbot malware to PUTILIN and others to be crypted.

60. Defendant MAKSIM GALOCHKIN (GALOCHKIN), aka BENTLEY, was a citizen and national of Russia. During the timeframe of this Indictment, GALOCHKIN was a

crypter, instructor, and tester for the Trickbot Group whose responsibilities included taking malicious files and testing them against known anti-virus programs to see if they were detected. Using the monikers "Bentley" and "Volhvb," among others known to the Grand Jury, GALOCHIKIN provided support and instruction to other members on encrypting files and loading malicious executable files.

61. Defendant, DMITRY PUTILIN (PUTILIN), aka GRAD, aka STAFF, was a citizen and national of Russia. During the timeframe of this Indictment, PUTILIN resided in Chelyabinsk, Russia, and used the online monikers "grad" and "staff." PUTILIN was a malware manager responsible for recruiting and hiring computer programmers to provide malware code for the Trickbot Group; procuring infrastructure for the Trickbot Group, such as servers, VPN and VPS providers; and testing Trickbot malware against counter anti-virus services.

62. Defendant SERGEY LOGUNTSOV (LOGUNTSOV), aka BEGEMOT, aka ZULAS, was a citizen and national of Russia. During the timeframe of this Indictment, LOGUNTSOV resided in St. Petersburg, Russia, and used the online monikers "begemot" and "Zulas." LOGUNTSOV was a developer for the Trickbot Group, overseeing the creation of code used to document, maintain, and control infected computers in the Trickbot botnet and of spamming software used by the Trickbot Group to infect other computers.

63. Defendant MAX MIKHAYLOV (MIKHAYLOV), aka BAGET, was a citizen and national of Ukraine. During the timeframe of this Indictment, MIKHAYLOV resided in Crimea. MIKHAYLOV was a malware developer for the Trickbot Group, responsible for developing remote networking code that allowed the Trickbot Group to remotely control infected victim computers used by the Trickbot Group. MIKHAYLOV also assisted with the development of Diavol ransomware.

64. Defendant MAKSIM RUDENSKY (RUDENSKY), aka FONIN, aka BINMAN, was a citizen and national of Russia. During the timeframe of the Indictment, RUDENSKY resided in St. Petersburg, Russia, and used the online monikers "fonin" and "binman." RUDENSKY was a Malware Developer for the Trickbot Group, overseeing the creation of Trickbot's web injection, browser password grabber and bot creation codes, among others. RUDENSKY authored and provided manuals to the Trickbot Group regarding the management of bots on the Trickbot botnet.

65. Defendant VALENTIN KARYAGIN (KARYAGIN), aka GLOBUS, was a citizen and national of Russia. During the timeframe of this Indictment, KARYAGIN was a malware developer. As a developer, KARYAGIN wrote code that supported ransomware and remote access capability. Using the moniker "Globus," KARYAGIN posted completed projects on the Trickbot Group's GitLab server and worked to develop and support the group's Diavol ransomware and backdoor capabilities.

66. Defendant MAKSIM KHALIULLIN (KHALIULLIN), aka MAXFAX, aka MAXHAX, aka KAGAS, was a citizen and national of Russia. During the timeframe of this Indictment, KHALIULLIN resided in Chelyabinsk, Russia, and used the online monikers "maxfax," "maxhax," and "kagas." KHALIULLIN was a malware manager and had roles and responsibilities in the Trickbot Group similar to PUTILIN.

CO-CONSPIRATORS

67. Co-Conspirator Vladimir Dunaev (Dunaev), aka ffx, aka tunri, named but not charged herein, was a citizen and national of Russia. At all times relevant to this Indictment until on or about June 1, 2021, Dunaev resided in the Yakutsk region of Russia and in Southeast Asia. Dunaev was a Malware Developer for the Trickbot Group, overseeing the creation of

internet browser injection, machine identification and data harvesting code used by the Trickbot malware.

68. Co-Conspirator Alla Witte (Witte), aka max, named but not charged herein, was a citizen and national of Latvia. At all times relevant to this Indictment until on or about February 4, 2021, Witte resided in Suriname. Witte was a malware developer for the Trickbot Group, overseeing the creation of code related to the monitoring and tracking of authorized users of the Trickbot malware, the control and deployment of what would later be known as "Diavol ransomware;" obtaining payments from ransomware victims; and developing tools and protocols for the storage of credentials stolen and exfiltrated from computers infected by the Trickbot malware.

69. Co-Conspirator 8 (CC8) was an organizer who managed the hiring, payment, and development of the Trickbot Group through the use of Jabber servers, GitLab accounts, and cryptocurrency wallets used for illicitly obtained criminal proceeds.

70. Co-Conspirators 9, 10, 11, and 18 (CC9, CC10, CC11, and CC18) were malware developers and computer programmers for Trickbot.

71. Co-Conspirators 14 and 15 (CC14 and CC15) were crypters who encrypted Trickbot malware to prevent its detection by anti-virus software.

72. Co-Conspirators 16 and 17 (CC16 and CC17) were spammers who deployed Trickbot malware through spamming, phishing and spear-phishing campaigns.

COUNT 1
(Conspiracy to Commit Computer Fraud and Aggravated Identity Theft, 18 U.S.C. § 371)

The Grand Jury charges:

73. Paragraphs 1 – 72 of this Indictment are hereby re-alleged and incorporated by reference as if fully set forth herein.

The Conspiracy

74. From in or around November 2015 through the date of this Indictment, in the Northern District of Ohio, Eastern Division and elsewhere, Defendants MIKHAIL TSAREV, aka MANGO; ANDREY ZHUYKOV, aka ZHUIKOV, aka DIF, aka DEF, aka DEFENDER; MAKSIM GALOCHKIN, aka BENTLEY; DMITRY PUTILIN, aka GRAD, aka STAFF; SERGEY LOGUNTSOV, aka BEGEMOT, aka ZULAS; MAX MIKHAYLOV, aka BAGET; MAKSIM RUDENSKY, aka FONIN, aka BINMAN; VALENTIN KARYAGIN, aka GLOBUS; and MAKSIM KHALIULLIN, aka MAXFAX, aka MAXHAX, aka KAGAS and others known and unknown to the Grand Jury, did knowingly and intentionally combine, conspire, confederate and agree to violate the laws of the United States, namely:

a. to intentionally access a computer without authorization and thereby obtain information from a protected computer and the offense was committed for purposes of commercial advantage and private financial gain, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(i);

b. to knowingly and with intent to defraud, access a computer without authorization and by means of such conduct further the intended fraud and obtain something of value, specifically, money, in excess of $5,000 in a one-

year period, in violation of Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A);

c. to knowingly cause the transmission of a program, information, code, and command and, as a result of such conduct, intentionally cause damage without authorization to a protected computer and the offense caused loss to one or more persons during a one-year period aggregating at least $5,000, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B);

d. to knowingly cause the transmission of a program, information, code, and command and, as a result of such conduct, intentionally cause damage without authorization to a protected computer and the offense caused damage affecting ten or more protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B);

e. with intent to extort from a person money and other thing of value, to transmit in interstate and foreign commerce a communication containing a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, in violation of Title 18, United States Code, Sections 1030(a)(7)(C) and 1030(c)(3)(A); and

f. to knowingly possess, transfer, and use, without lawful authority, a means of identification of another person, during and in relation to felony violations of Title 18, United States Code, Sections 1030, 1343 and 1344, to wit, Computer

Fraud, Wire Fraud, and Bank Fraud, in violation of Title 18, United States Code, Section 1028A(a)(1).

Objects of the Conspiracy

75. The objects of the conspiracy included:

a. infecting victims' computers with Trickbot malware designed to capture victims' online banking login credentials;

b. obtaining and harvesting other personal identification information, including credit cards, emails, passwords, dates of birth, social security numbers, and addresses;

c. infecting other computers networked with the initial victim computer;

d. using the captured login credentials to fraudulently gain unauthorized access to victims' online bank accounts at financial institutions;

e. stealing funds from victims' bank accounts and laundering those funds using U.S. and foreign beneficiary bank accounts provided and controlled by Trickbot Conspirators; and

f. facilitating the infection of victims' computers with ransomware.

Manner and Means of the Conspiracy

It was part of the conspiracy that:

76. Each defendant provided specialized skills and filled specific roles in furtherance of the conspiracy. For example, some defendants recruited and advertised for computer programmers to develop the Trickbot malware, mostly on Russian-based freelancing and employment websites.

77. Defendants and their co-conspirators required potential recruits to demonstrate their computer programming abilities and suitability for the conspiracy by assigning potential recruits computer programming tests designed to facilitate aspects of the Trickbot malware, including the use of web injects.

78. Defendants and their co-conspirators then provided those computer programmers that demonstrated sufficient proficiency with credentials to access a private communication server through which the Trickbot Group distributed and received communications related to the development, maintenance, and deployment of Trickbot.

79. Defendants and their co-conspirators developed and updated the Trickbot malware that, when installed on an infected computer, was designed to both receive commands and send information from the infected computer back to Defendants.

80. Defendants and their co-conspirators crypted Trickbot to evade detection by anti-virus software and other protective measures used by victims.

81. Defendants and their co-conspirators leased access to servers from legitimate hosting companies using false and fictitious names. These servers were used to deploy, maintain, and manage the use of the Trickbot malware.

82. Defendants and their co-conspirators spread Trickbot through a campaign of spamming, phishing, and spear phishing. Defendants designed the emails used in these campaigns to falsely represent that the emails were from legitimate companies, associations, or organizations.

83. Defendants and their co-conspirators crafted the phishing emails to fraudulently entice a victim to open an attachment, such as a business invoice, or click on a hyperlink that falsely represented itself to be legitimate. When the victim clicked on the attachment or

hyperlink, the victim's computer was typically infected by Trickbot malware either embedded in the attachment or on a malicious domain connected to the hyperlink, without the victim's consent, knowledge, or authorization.

84. Defendants and their co-conspirators designed Trickbot to determine if the victim computer was connected to other computers on a network and then infect other computers to which the victim computer had access.

85. Defendants and their co-conspirators designed Trickbot to automate the theft of confidential personal and financial information, including online banking credentials, by monitoring the victims' use of their computers and then using keylogging or web injects to surreptitiously obtain and trick a user to enter personal and financial information.

86. Defendants and their co-conspirators used keystroke logging to steal victims' online banking credentials when the victims logged into their online bank account from their infected computers.

87. Defendants and their co-conspirators also used web injects to display false online banking pages on the victims' web browsers that captured online banking information as the victims entered it and then transmitted the captured data back to Defendants.

88. Defendants and their co-conspirators used the confidential personal and financial information obtained by Trickbot to falsely represent to banks and financial institutions that Defendants and other Trickbot Conspirators were the victims or employees of the victims and were authorized to access the victims' bank accounts and make electronic funds transfers from the victims' bank accounts.

89. Defendants and their co-conspirators then used the captured online banking credentials to pose as the victim and cause banks and financial institutions to make and attempt

to make unauthorized wire transfers, ACH payments, or other electronic funds transfers from the victims' bank accounts, without the knowledge or authorization of the account holders.

90. Defendants and their co-conspirators wrote and employed computer programs that used stolen personal identification information to purchase goods from online stores and ship the products to physical addresses.

91. Defendants and their co-conspirators then used money mules to receive the wire transfers, ACH payments, and other electronic funds transfers from the victims' bank accounts.

92. Defendants and their co-conspirators then directed and caused the money mules to further transfer the stolen funds to be placed under the control of other members of the conspiracy.

93. Defendants and their co-conspirators subsequently began deploying malware, including Diavol, Conti, and Ryuk.

94. The group infected computers, communicated with, and extorted victims using the Diavol, Conti, and Ryuk ransomware variants.

95. In order to achieve the objects of this conspiracy, Defendants and their co-conspirators relied on several manners and means to evade detection by both victims and law enforcement. These efforts included:

a. using pre-paid credit cards, false credentials, and cryptocurrency to pay for servers, domains, VPNs, and other infrastructure;

b. using multiple proxies to communicate, including the C2 server, infected computers, commercial VPNs, and commercial proxies;

c. communicating over an encrypted private messaging server;

d. using different monikers when communicating over different channels;

e. regularly moving infrastructure and changing communication channels to avoid detection;

f. using U.S.-based and foreign money mules;

g. using cryptocurrencies including bitcoin to surreptitiously facilitate the transfer of funds; and

h. using cryptocurrency mixers to hide the origins and destinations of cryptocurrency.

Overt Acts

96. In furtherance of the conspiracy and to affect the objects thereof, Defendants and others known and unknown to the Grand Jury, did commit and cause to be committed the following overt acts in the Northern District of Ohio, Eastern Division and elsewhere.

I. DEVELOPMENT, ADMINISTRATION, AND MAINTENANCE OF TRICKBOT

A. TRANSITION FROM DYRE GROUP TO TRICKBOT GROUP

97. On or about November 11, 2015, PUTILIN obtained credentials to a private server used by the operators of the Dyre malware. PUTILIN and others transitioned their operation to the creation of a new malware based on the Dyre framework.

98. Beginning no later than on or about December 4, 2015, PUTILIN began communicating with the Trickbot Group about providing administrative support to the Trickbot team, including recruiting other computer programmers and leasing server space on which to develop, deploy, and maintain the Trickbot malware.

B. ACQUIRING SERVERS AND VPN AND VPS SERVICES

99. Beginning no later than in or around June 2015 and continuing through in or around April 2019, PUTILIN used a PayPal account under his control to purchase VPN and VPS services from numerous hosting and anonymization companies in the United States, United

Kingdom, Lithuania, Canada, Italy, Russia, the Netherlands, and elsewhere, initially for the Dyre group and later for the Trickbot Group.

100. On or about December 7, 2015, PUTILIN and other Trickbot Conspirators agreed that PUTILIN would continue providing support services for Trickbot's development and maintenance and that he would continue "testing software" and "installing virtual machines."

101. On or about December 7, 2015, PUTILIN discussed with CC8 the need to rebuild their infrastructure following the collapse of the Dyre network as follows:

CC8	You owe nothing to anyone; we just need to restore our work
PUTILIN	Everything got disrupted in one second
CC8	We are restoring everything bit by bit
PUTILIN	Yes, it is hard work, but I am sure everything will be restored. Thank you again. I will do some work now.
PUTILIN	I hope that everything will go through fine. A question about work -- can I order servers in advance? To avoid this rush
CC8	yes, that is how it will be
CC8	the rush is now because of the technical collapse

102. On or about December 9, 2015, PUTILIN agreed to rent servers that accepted "Paymer" checks[3] for the Trickbot Group and then provide those servers to members of the Trickbot Group.

103. On or about December 9, 2015, PUTILIN agreed with other Trickbot Conspirators that he would register each server under a different account and email, to achieve this he used over 100 different email accounts provided by a co-conspirator to achieve this goal.

104. On or about December 9, 2015, CC9 provided ZHUYKOV with a URL to the administrative area of what would become a Trickbot development server. CC9 requested

---

[3] Paymer is an electronic software and hardware system designed to manage payment obligations in the form of electronic checks which are payable to the "bearer." Paymer was based in Russia.

ZHUYKOV help set up the server and organize the users into three groups: the "pr" or "proger" group who would not be visible to each other by default unless they added each other; the "main" group who could see each other but not the progers; and lastly, a group consisting of CC8, CC9, and one other Trickbot Conspirator who would be able to see and be seen by everyone on the server. CC9 told ZHUYKOV to help CC9 set these groups up and instructed ZHUYKOV not to store anything on ZHUYKOV's computer and to encrypt any information from the server. CC9 told ZHUYKOV he only would be an administrator temporarily because he would be needed as a designer and a proger.

105. On or about December 11, 2015, PUTILIN purchased servers based in Russia for the Trickbot Group. Later that same day, CC9 instructed PUTILIN not to buy servers in Russia anymore and instead purchase them from other European countries.

106. Throughout 2016, PUTILIN maintained a detailed record of server specifications, leases and payments for servers he and others acquired for the development, maintenance, and deployment of Trickbot.

107. Beginning in or around January 2016, PUTILIN and KHALIULLIN began discussing the need to acquire "fullz," meaning the full identifiers to include names, dates of birth, social security numbers, and other identifiers of Americans to conduct fraud on banks.

108. On or about January 22, 2016, CC9 provided ZHUYKOV credentials to a Jabber server and told ZHUYKOV he could administer the server. This made ZHUYKOV responsible for managing new and existing communication accounts used by members of the group.

109. On or about February 1, 2016, PUTILIN and KHALIULLIN discussed the need to use an American server in their quest to obtain "fullz" so that "no one will discover that we are from Russia."

110. On or about February 2, 2016, KHALIULLIN told PUTILIN, "They should say thank-you to us that we are stealing money from the Americans we should get the Medal of Valor," to which PUTILIN replied, "exactly."

111. On or about February 9, 2016, CC9 provided ZHUYKOV credentials to a new server for the Trickbot Group.

112. On or about February 29, 2016, PUTILIN introduced KHALIULLIN to CC8, a leader of the Trickbot Group, in order for KHALIULLIN to begin acquiring servers on behalf of the group. PUTILIN also noted that CC9, CC10, and CC11 were "employees" of the Trickbot Group.

113. Beginning no later than in or around July 2016 and continuing through in or around December 2018, KHALIULLIN used a PayPal account under his control to purchase VPN and VPS services from numerous hosting and anonymization companies in the United States, Canada, Russia, the Netherlands and elsewhere, for the Trickbot Group.

C. MANAGEMENT OF THE TRICKBOT GROUP

114. From at least July 2016 until the time of this Indictment, the Trickbot Group employed several members who served as mid-level managers below CC8. TSAREV, PUTILIN, and RUDENSKY all functioned in this role. TSAREV managed finances and coordinated operational activities with other individuals. TSAREV regularly received reports from other members, paid members, and provided updates on recent activities to group leadership. One of TSAREV's primary roles was paying salaries of group members.

115. In a chat on or about October 10, 2020, TSAREV described his role with a co-conspirator, CC15, as follows: "So in a nutshell-I'm something like a manager between tenants

and coders, I solve the misunderstandings that have arisen, I'm looking for what the team needs (routers, shells, crypts, etc.), so if you have any questions, you can contact me."

116. On or about July 16, 2021, TSAREV wrote to CC8 reporting that the "core team of coders" numbered 62 with 6 new coders to join. The communication further described the need to pay 3000 for expenses and other needs totaling a budget of "164.8k just a month."

D. HIRING COMPUTER PROGRAMMERS TO PROVIDE CODE FOR THE TRICKBOT MALWARE SUITE

117. Beginning no later than in or around November 2015, the Trickbot Group began recruiting new programmers to rebuild its infrastructure following the purported Russian action against the Dyre group.

118. In or around January 2016, LOGUNTSOV agreed to work for and join the Trickbot Group.

119. On or about February 29, 2016, PUTILIN introduced KHALIULLIN to CC8, a leader of the Trickbot Group, in order for KHALIULLIN to begin recruiting computer programmers on behalf of the group.

120. On or about May 3, 2016, PUTILIN, CC8 and CC9 agreed to purchase fee-based access to Russian and Belarussian-based job websites to gain access to resumés for computer programmers looking for employment.

121. Beginning no later than in or around March 2016, Defendants devised a recruitment notice for computer programmers to be used on a computer game website to search for potential malware developers.

122. Beginning no later than in or around March 2016, Defendants created a notice for a Russian-language job website that required potential applicants to demonstrate their computer

programming skills by completing a "test" coding task, which required them to successfully program a web inject or other components necessary for the operation of Trickbot.

123. On or about May 4, 2016, and May 16, 2016, PUTILIN created email accounts to create accounts on job-listing websites and to use these accounts to communicate with potential recruits to the Trickbot Group.

124. On or about June 30, 2016, PUTILIN and CC9 discussed the wording of a recruitment posting on the Russian-based job website. CC9 advised PUTILIN not to use the word "inject" in a job posting for a computer programmer because it was "dangerous" and because CC9 was concerned that posting for "crooked vacanc[ies]" are "likely to get us caught." In the same conversation, CC9 instructed PUTILIN to "go ahead" and post the job posting.

125. On or about July 26, 2016, KHALIULLIN told PUTILIN that a potential job candidate refused to complete the Trickbot test and stated, "a job applicant states that Chrome is a licensed software and it is illegal to alter, decompile, or change the source code for it. He ask if they are talking about Chromium browser."

126. On or about July 26, 2016, PUTILIN responded to KHALIULLIN's message and stated, "Yes[.] We are sorry for this error[.] We are talking specifically about Chrome. The job is not totally legal, but everything is very confidential and is executed via Jabber OTR, an encrypted communication platform. Be assured that all the work will be paid for and your activities will be safe. We have been working in this field for five years. [] Either way, it's up to you. We are waiting for your reply."

127. On or about July 7, 2016, CC9 instructed PUTILIN how to create a recruitment notice for a computer programmer for the Trickbot Group, including how to assess the computer

programming test assigned to the recruit. CC9 further instructed PUTILIN only to talk directly to potential recruits about the injection code.

128. On or about May 17, 2016, PUTILIN used an email account created and controlled by the Trickbot Group to contact RUDENSKY and separately sent RUDENSKY an email from the Russian-language job site to send RUDENSKY a test task for the Trickbot Group.

129. On or about May 19, 2016, RUDENSKY received the test task but later withdrew from consideration due to technical problems with code for an internet browser.

130. In or around July 2016, RUDENSKY applied for two additional positions with the Trickbot Group and received test tasks for both vacancies.

131. On or about July 19, 2016, RUDENSKY sent an email to the Trickbot Group to an account created and controlled by the Trickbot Group stating RUDENSKY was having problems with the test task. That same day, PUTILIN provided RUDENSKY's response to CC8.

132. On or about July 21, 2016, RUDENSKY completed the task and sent the response to the Trickbot Group. In the email, RUDENSKY noted that the program should be checked "when the antivirus is off as it can get angry with 'injections' during the process." Attached to the emails were programs that modified the Google Chrome internet browser to enable the Trickbot Group to modify the HTTP GET and POST information from the browser and inject information into the internet session. This type of program was required for the Trickbot malware to intercept and harvest online credentials.

133. On or about July 25, 2016, PUTILIN and CC8 discussed RUDENSKY's application and completion of the test task. During the conversation, PUTILIN and CC8 noted that their test tasks were considered "blackhat" hacking. The text of the conversation follows:

CC8	[RUDENSKY]
CC8	[RUDENSKY] did the test task
CC8	Who else did it?
CC8	Why are you communicating with this one
CC8	[RUDENSKY] wrote to you
CC8	The main reason is that this functionality can be used for illegal activities/ blackhat (formgrabbing, injects) I do not do Blackhat
CC8	plus, [RUDENSKY] did not even do the test task
PUTILIN	Later [RUDENSKY] changed his mind and [RUDENSKY] is ready to write in the evening. There is nothing to lose if [RUDENSKY] writes, right?
PUTILIN	Is [RUDENSKY's] test task being checked?
CC8	let him create a Jabber
CC8	I will contact him there
CC8	until people finish the test task, do not exchange any Jabbers
CC8	We need to stop communicating with idiots
PUTILIN	We are not in the main one, but in the external one. I got it.
CC8	it does not matter, they sent the test task
PUTILIN	in short, describe the question they are asking, so I don't have to bother you later
CC8	If there is no result, we don't communicate any more
PUTILIN	The majority understand that this is blackhat and asking for the commercial target .
CC8	if they ask additional questions, this person is not suitable
CC8	This is the gist

Later that same day, PUTILIN and CC8 continued the conversation as follows:

CC8	Anyhow, send as many messages to programmers as possible
CC8	50 per day to the new ones
CC8	[KHALIULLIN] is already doing a good job) there are a lot of people
CC8	We'll find several decent programmers

134. On or about July 25, 2016, RUDENSKY obtained credentials to a private Trickbot Group communications server.

135. On or about May 27, 2016, PUTILIN used an email account created and controlled by the Trickbot Group to email Co-Conspirator Vladimir Dunaev, aka ffx, aka tunri and present him with a test task for the Trickbot Group.

136. On or about May 29, 2016, Dunaev completed and returned the first Trickbot Group test task, which required him to write a server application that simulates a SOCKS server[4].

137. On or about May 30, 2016, PUTILIN used an email account created and controlled by the Trickbot Group to ask Dunaev to complete a second task involving altering a Firefox browser.

138. On or about June 1, 2016, Dunaev completed the Firefox browser alteration and provided a Dropbox URL linked to the completed task to PUTILIN.

139. On or about June 2, 2016, PUTILIN provided Dunaev's Dropbox URL to CC9. After CC9 reviewed the code, CC9 and PUTILIN engaged in the following conversation concerning Dunaev:

CC9	It's all working.
CC9	It's all correct.
CC9	The guy did the job.
PUTILIN	F-----g awesome.)
PUTILIN	What are we doing now?
CC9	I'll ask now.
CC9	They'll respond and we'll knock at that guy's door until we get him.
CC9	It seems like he's great.
CC9	He can do both this kind of stuff and that kind.
CC9	What is needed.
CC9	Tell the guy that we tested it and the assignment works.
CC9	Everything's fine with that.
CC9	Consider him hired.

[4] SOCKS is a protocol on the internet that defines the method in which internet resources are requested from one computer to another. A SOCKS server would request data and then route the information back to the client.

CC9	Just need to come to an agreement with [CC8]...
CC9	where we should put him.
PUTILIN	Maybe write to him about Jabber for now?
CC9	No.
CC9	Nothing for now.
PUTILIN	Well and also tell dif, so that he registers [him].
CC9	No.
PUTILIN	Okay.
CC9	We'll manage it ourselves.
CC9	Just on pause for now.
PUTILIN	But otherwise everything is f-----g great.
CC9	Say that the boss is on a trip, but that everything is great.
CC9	He passed the test.
CC9	We have another Jabber

Later that same day, PUTILIN and CC9 continued the conversation as follows:

CC9	He's capable of everything.
CC9	Such a person is needed.
PUTILIN	I'm afraid that he can tell the firm to go hell, or ask for more money.
PUTILIN	Well that's something for the leadership to decide.
CC9	His assignment is the usual kind.
CC9	There's nothing strange in it.
CC9	:)
PUTILIN	So he's going to develop programs?
CC9	Well, yeah.
PUTILIN	Well, in that case, that's f-----g great.

140. Following this conversation, PUTILIN and CC9 provided Dunaev with credentials and information to join the Trickbot Group and its private communication server.

141. In or around the summer of 2015, ZHUYKOV responded to a job posting seeking programmers. After successfully completing test tasks, ZHUYKOV was invited to a meeting at an office in Sochi, Russia.

142. Thereafter, on or about July 24, 2015, ZHUYKOV was provided credentials to a development server where he had a conversation with CC18. During the conversation, CC18 instructed ZHUYKOV on various methods to avoid detection. Specifically, CC18 told

ZHUYKOV he should be using a proxy or a VPN in the United States or Europe when doing work tasks or testing.

143. From beginning at least in or about in November, 2016 until the time of this Indictment CC18 and ZHUYKOV discussed developing a script that would search online stores, order goods with stolen personal identifying information, checkout and then arrange to have the goods delivered to specified addresses. ZHUYKOV indicated specific websites he was using to check on the status of the proxy servers, but CC18 told ZHUYKOV to never check on shared resources because they (the proxies) would be immediately killed and zapped.

144. From beginning at least in or about in November 2016 until the time of this Indictment, CC18 provided ZHUYKOV a list of proxy IP addresses and indicated that they would work. CC18 told ZHUYKOV there were a few points he needed to follow for his safety.

145. From beginning at least in or about in November 2016 until the time of this Indictment, these points included not going to personal accounts from the development system he was using, always making sure to login with VPN and using the Ubuntu operating system. CC18 suggested ZHUYKOV make a disk partition on his computer so he could work on it and not to include any personal information on it. CC18 then provided ZHUYKOV with personal identifying information from eight individuals and indicated they would be the "payers" and "buyers" when ordering goods online. The data provided to Zhukov included names, phone numbers, dates of birth, social security numbers, addresses, and credit card numbers.

146. On or about January 26, 2016, ZHUYKOV and CC9 engaged in the following conversation concerning development of the Trickbot malware:

CC9	The group name is "test1."
CC9	The client's version must be partially indicated as well.
CC9	Did you get it? Did you get how to format URL?
CC9	You can use PHP, Perl to create generator.

CC9	Particular number of lines
CC9	with different IP
CC9	Hosts.
ZHUYKOV	Can you give me an example?
ZHUYKOV	I need to leave for an hour. Will you be here?
CC9	No
CC9	I need this tomorrow
CC9	Evening.
CC9	[URL]
CC9	This an example
CC9	Of request
CC9	See above.
CC9	I need 100k of those

147. From no later than in or around February 2016 through the date of this Indictment, LOGUNTSOV provided computer code and technical support used in the development and maintenance of the Trickbot malware, including developing code that allowed the Trickbot Group to assign unique identifiers to infected victim bots, manage and control infected victim bots and also writing code that facilitated spamming campaigns meant to infect victim computers with Trickbot malware.

148. On or about February 15, 2016, ZHUYKOV and CC9 engaged in the following conversation concerning creating a site to hire testers for Trickbot:

CC9	We need to create site
CC9	hiring site for freelancers.
CC9	Any ideas?
ZHUYKOV	What outcome you expect from this site?
CC9	We need to find gameaholics.
CC9	The site will be a business card
CC9	With possibility to leave a request.
CC9	Active vacancies…
CC9	happy freelancers
CC9	and all that.
CC9	We need to find such a site,
CC9	make a copy of it.
ZHUYKOV	What kind of gameaholics?

CC9	The people who spends all day at comp.
ZHUYKOV	Do you mean who plays game or play for money?
CC9	We need those people for particular tasks.
ZHUYKOV	I see.
CC9	Not to play games of course
ZHUYKOV	As testers?
CC9	Yes
CC9	Kind of.
CC9	With the pretext of testing games.
ZHUYKOV	I see.
CC9	To make some money.
CC9	It's a creative task.

149. On or about March 8, 2016, ZHUYKOV and CC9 engaged in the following conversation concerning storage space needed for the Trickbot Group's git storage backup:

CC9	Hi
CC9	Could you take a look on git storage?
CC9	Did it explode yet?
CC9	:-D
CC9	It's off now
ZHUYKOV	No. A little more than 7 GB will take all room storage.
ZHUYKOV	Today's full backup took 10 GB of storage. There is no room left. We need to pay an account.

150. On or about July 26, 2016, shortly after RUDENSKY received credentials to the private Trickbot communications server, RUDENSKY provided a file called "injector/module.rtf" to the Trickbot Group.

151. This file provided guidance to the Trickbot Group describing how the malware would monitor the activity on infected computers and insert web injects into internet browser sessions.

152. On or about July 26, 2016, RUDENSKY provided a file to the Trickbot Group called "injector/inj.rtf", which provided instruction to Trickbot Conspirators instructing how to configure the injection files in the Trickbot malware.

153. On or about July 27, 2016, RUDENSKY provided code to be used in the Trickbot malware to the Trickbot Group, specifically a program called "splice.dll" that related to the use of web injects and was critical to the operation of the Trickbot malware.

154. On or about and between July 28, 2016, and June 1, 2018, RUDENSKY and other Trickbot Group members modified and updated the splice.dll code approximately 104 times, each update and modification consisting of a separate overt act.

155. On or about July 27, 2016, RUDENSKY provided code for the main Trickbot browser engine injection program, specifically focused on the Google Chrome browser, to the Trickbot Group.

156. On or about and between July 27, 2016, and the date of this Indictment, RUDENSKY and other Trickbot Group members modified and updated the browser engine injection code for Google Chrome browser approximately 700 times, each update and modification consisting of a separate overt act.

157. On or about September 3, 2018, RUDENSKY provided code to the Trickbot Group for a module that allowed Trickbot malware to harvest stored passwords in web browsers and export them back to the Trickbot Group.

158. On or about September 3, 2018, and continuing through the date of this Indictment, RUDENSKY and other Trickbot Group members modified and updated the above-described password harvesting module code approximately 150 times, each update and modification consisting of a separate overt act.

159. On or about the dates listed below, RUDENSKY submitted for counter anti-virus checks the above-described password harvesting module code to determine if anti-virus software would detect the code, each submission consisting of a separate overt act:

a. April 30, 2019;

b. May 3, 2019; and

c. September 12, 2019.

160. On or about and between February 24, 2017, and November 15, 2018, RUDENSKY provided and updated a file called "bot/cs2 proto.rtf" to the Trickbot Group. This file provided guidance on the function and management of infected bots in the Trickbot botnet.

161. On or about September 19, 2016, LOGUNTSOV communicated with a Trickbot co-conspirator regarding the provision of code needed for the Trickbot malware.

162. On or about September 26, 2016, LOGUNTSOV forwarded code used for the Trickbot malware to the Trickbot Group.

163. On or about and between September 27, 2016, and October 2, 2016, LOGUNTSOV corrected a coding error in the Trickbot malware that affected Trickbot's ability to identify and control infected computers (bots) in the Trickbot botnet and provided the corrected code to other members of the conspiracy.

164. On or about November 14, 2016, PUTILIN obtained a copy of a file called "test системы" ("system test") from the Trickbot Group. This file was used for web injections and contained approximately 30 individual online banking URLs followed by an IP controlled by the Trickbot Group, which were later used by the Trickbot malware to trick victims into entering their banking credentials into spoofed banking websites controlled by the Trickbot Group.

165. On or about November 17, 2016, PUTILIN submitted the "test системы" file to an online counter anti-virus checker to determine if the program would be detected by anti-virus software.

166. On or about February 10, 2017, LOGUNTSOV provided computer code for the purpose of developing a phishing and spam server used for the creation and management of malicious spam to the Trickbot Group.

167. No later than on or about March 6, 2017, PUTILIN and others obtained an account with an online counter anti-virus service, for the purpose of testing the Trickbot malware against various anti-virus software.

168. No later than on or about December 11, 2017, MIKHAYLOV gained access to the Trickbot development server.

169. From on or about December 11, 2017, through and including the date of this Indictment, MIKHAYLOV provided coding support to develop a remote control module to allow the Trickbot Group to control a victim computer over the internet.

170. On or about March 10, 2018, the Trickbot Group registered an account with a counter anti-virus checker that was advertised on well-known underground cybercriminal forums.

171. Between or around March and October 2018, the Trickbot Group uploaded approximately over 43,000 files to the counter anti-virus checker. Some of the files had names that suggested being used in financial fraud schemes such as "HSBC_deposit_Confirmation-0," "paypal" and "Bankline_Secure_Message."

172. On or about April 3, 2018, RUDENSKY modified and provided a technical document concerning Trickbot's operation to the Trickbot Group.

173. On or about October 2, 2018, Co-Conspirator Witte gained access to the Trickbot development server.

174. On or about October 11, 2018, Witte provided code used to manage and track authorized users of the Trickbot malware to the Trickbot Group.

175. On or about December 17, 2018, Witte created and provided to the Trickbot Group a video demonstrating how to use the Trickbot user tracking software.

176. On or about May 6, 2019, LOGUNTSOV provided additional development and support for the Trickbot code used to track and control infected computers to the Trickbot Group.

177. On or about and between August 19, 2019, and the date of this Indictment, RUDENSKY and other Trickbot Group members created and modified "injector/Logs60.rtf," which was a file that explained to members of the conspiracy how to exploit HTTP POST and HTTP GET information.

178. On or about and between October 2019 and continuing through on or about January 2021, Co-Conspirator Witte provided code to the Trickbot Group to operate and deploy Diavol ransomware.

179. On or about January 14, 2020, Co-Conspirator Witte conducted internet searches for "laravel faker bitcoin address," a reference to creating a fake Bitcoin address to use to test the Diavol ransomware payment system.

180. On or about and between June 1, 2016 and June 1, 2021, Co-Conspirator Dunaev provided, modified and updated malware code related to the following projects for the Trickbot Group, each modification or update consisting of a separate overt act:

a. **firefox_pseudo** - Modification of Mozilla source code to develop a custom Firefox browser called pseudobrowser/superbrowser.

b. **grabber** - Grabs browser data including browser history, HTTP cookies, HTML5 local storage, and Flash Local Shared Objects/LSO (Flash cookies) from Internet browsers and saves them to an autogenerated configuration file.

c. **import** - Imports and loads stolen browser profile data including browser cookies, history, local storage, and Flash LSO into the superbrowser.

d. **launcher** - A program used to launch the superbrowser application with specified browser profiles to auto-login to online accounts.

e. **getKey** - A hash generator program that generates a machine key or hash based on a computer's hardware to uniquely identify a Trickbot operator's machine for use with the superbrowser.

f. **patcher** - A program that implements browser protection for the superbrowser by patching the superbrowser with a unique key/hash to prevent unauthorized copying, distribution, and use.

g. leveldb - Utilized by the grabber program, LevelDB is a fast key-value database storage library built by Google that can be used by a web browser to store a cache of recently accessed web pages.

h. **snappy** - Google's data compression and decompression library utilized by the grabber program.

181. From beginning at least in or about in November 2016 and continuing until the time of this Indictment, GALOCHKIN was a crypter. In multiple cases, GALOCHKIN obtained a list of "loaders" and "bots", which were likely used for testing purpose to ensure malware could penetrate a machine undetected. In the example below, GALOCHKIN received "loader"

and "bot" IP addresses from another group member. It is believed that these IP addresses were used to load malware onto bots for testing.

182. On or about August 17, 2020, GALOCHKIN received a list of loaders and bots to test, and a day later GALOCHKIN responded with a download link for a site the group used to host data. This site was observed in several chats with group members and it is believed to be used primarily as a file sharing site to send various files between members. Based on the initial message, it is believed that the download link contained the working or "crypted" malware files that passed the testing process.

183. From beginning at least in or about in November 2016 until the time of this Indictment, GALOCHKIN was also involved in providing support on a variety of projects within the group. In a message to CC8, GALOCHKIN indicated he was involved in supporting a variety of activities including file encryption, trick dlls[5] (likely Trickbot dll files), and was also providing instructions to other team members:

CC8	Hello. How are you? Whater are your results? What are the challenges? What ideas do you have that can be added and improved?
GALOCHKIN	Everything is well. Interesting and rich. All cryptors have switched from manual labor to automatic assembly through a build machine. Now they are bust updating and cleaning stubs. And I make files on the build machine, check and issue. If something is being built dirty, I turn to the cryptor. He cleans the stub. Check again and release. Tasks: 1. Encrypt files for Leo on the build machine. 2silkcode Coba\t 3.Lockers

[5] A DLL, which stands for Dynamic Link Library, is a shared program module or library that contains code and data that can be dynamically called by a Windows executing program during run time. It can be used by more than one Windows's program at the same time.

	4. Cobalt exe and dll 5. Dll trika 6. I teach and provide other team members with access to the build machine so that they can collect crypts themselves. 7. Preparing links for loading and testing emails for netwalker, hash, cherry.

184. On or about May 5, 2021, an administrator from a different malware group used a Trickbot Group messaging server to communicate with MAKSIM GALOCHKIN, aka BENTLEY. The administrator asked BENTLEY for access to a known cybercriminal forum. BENTLEY provided the administrator with a username and password to access the forum.

185. From beginning at least in or about in November 2016 until the time of this Indictment, GALOCHKIN sent regular reports to TSAREV detailing his crypting efforts. These reports provided summaries of the various executables and files he had been working on.

186. Between on or about June 3, 2021, and on or about September 6, 2021, GALOCHKIN sent TSAREV ten updates on the progress of cryptors for several Trickbot Group build machines.

187. On or about June 10, 2021, GALOCHKIN provided technical advice to a Trickbot Group member regarding how to evade detection of a document that had been flagged for security issues by an anti-virus program.

188. On March 23, 2020, email addressed directly linked to KARYAGIN provided revisions to work products on the Trickbot Group-controlled GitLab server and the name VALENTIN KARYAGIN as the name of the person committing to the job. The author name was listed as "globus." Subsequent revisions to these work products kept the same author name but also displayed it as the committer instead of KARYAGIN's full name. Subsequent revisions were made using the moniker "globus," which is consistent with the moniker utilized by KARYAGIN.

189. On or about January 14, 2020, and May 18, 2020, KARYAGIN communicated with MIKHAYLOV and Co-Conspirator Witte on a Trickbot communication server about bot registration and details of the Diavol ransomware. Specifically, KARYAGIN communicated with Co-Conspirator Witte that he was writing functionality in the Cryptolocker project that authorizes and registers a bot. KARYAGIN also solicited help from Witte to create a button on a site for registering bots so that he could view the POST request from the bot registration in its raw form.

190. From beginning at least in or about in November 2016 until the time of this Indictment, KARYAGIN also participated in developing malware loaders and software capable of manipulating running processes on victim machines. In collaboration with MIKHAYLOV and others, KARYAGIN developed the following projects on the GitLab server:

a. **morphcode32** - Encrypts and decrypts malicious code during execution, likely to evade antivirus detection.

b. **binary_server** - Program related to bazarloader/backdoor malware. The code in the project references "botleggers.png", the panel used for maintaining bots infected with bazarloader.

c. **Cryptolocker** –Ransomware project referred to as Enigma and Diavol.

d. **LightLoader_exe_dll** - Creates loader modules, aka droppers, for loading & running executable files on victim systems. Resolves Emercoin (.bazar) domains.

e. **LightBackDoor** - Creates backdoor/bot modules capable of executing malicious batch and PowerShell scripts, binaries, and killing running processes on victim systems.

f. **VNC** – Allows for the remote operation of another computer.

II. DEPLOYMENT OF TRICKBOT

191. Beginning no later than in or around October 2016 and from a location outside the United States, the Trickbot Group purchased and configured C2 servers that hosted malware and spam campaigns and web inject servers for spoofed bank websites, and began deploying Trickbot malware to victims throughout the world.

192. No later than on or about January 31, 2017, PUTILIN created and obtained a document entitled "спам", which was Russian for "Spam." The document contained detailed instructions that provided guidance for the following steps necessary for deployment:

a. First obtain Trickbot malware from ZHUYKOV;

b. Second, provide the Trickbot malware to CC14 and CC15, who would encrypt the malware to prevent its detection by anti-virus software; and

c. Third, provide the crypted malware to CC16 and CC17 to then deploy Trickbot through spamming, phishing and spear-phishing campaigns.

193. The Trickbot Group infected millions of victim computers worldwide, including in Russia, the United Kingdom, the United States, and the Northern District of Ohio, Eastern Division and elsewhere and gained unauthorized access to victim computers (1) for purposes of commercial advantage and private financial gain; (2) to obtain something of value, specifically, money, in excess of $5,000 in a one-year period; (3) to intentionally cause damage without authorization to a protected computer and the loss to one or more persons during a one-year period aggregated at least $5,000; (4) to cause the transmission of a program, information, code, and command and, as a result of such conduct, intentionally cause damage without authorization to a protected computer and the offense caused damage affecting ten or more protected

computers during a one-year period; (5) with intent to extort from a person money and other thing of value, transmitted in interstate and foreign commerce a communication containing a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion; and (6) to knowingly possess, transfer, and use, without lawful authority, a means of identification of another person, during and in relation to felony, each infection constituting a separate act in furtherance of the conspiracy, including the following:

Victim ID	Location	Approximate Dates of Infection
CW 1	Avon, OH	October 6 – 20, 2017
CW 2	Akron, OH	May 7, 2019
CW 3	North Canton, OH	October 2 – 3, 2018
CW 4	Ripon, CA	December 12, 2016
CW 5	Fort Myers, FL	March 30, 2018
CW 6	Bennington, VT	May 16, 2018
CW 7	Lynchburg, VA	September 24, 2018
CW 8	Eastland, TX	September 28, 2018
CW 9	Tulare County, CA	October 10, 2018
CW 10	New York, NY	December 7, 2018
CW 11	Minnesota	February 6, 2019

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

COUNT 2
(Conspiracy to Commit Wire Fraud and Bank Fraud, 18 U.S.C. § 1349)

The Grand Jury further charges:

194. The factual allegations of Paragraphs 1–72 and 97–193 of this Indictment are hereby re-alleged and incorporated by reference as if fully set forth herein.

195. From in or around November 2015 continuing through the date of this Indictment, in the Northern District of Ohio, Eastern Division and elsewhere, Defendants MIKHAIL TSAREV, aka MANGO; ANDREY ZHUYKOV, aka ZHUIKOV, aka DIF, aka DEF, aka DEFENDER; MAKSIM GALOCHKIN, aka BENTLEY; DMITRY PUTILIN, aka GRAD, aka

STAFF; SERGEY LOGUNTSOV, aka BEGEMOT, aka ZULAS; MAX MIKHAYLOV, aka BAGET; MAKSIM RUDENSKY, aka FONIN, aka BINMAN; VALENTIN KARYAGIN, aka GLOBUS; and MAKSIM KHALIULLIN, aka MAXFAX, aka MAXHAX, aka KAGAS and others known and unknown to the Grand Jury, did knowingly and intentionally combine, conspire, confederate and agree with each other to commit the federal offenses of Wire Fraud, which affected a financial institution and Bank Fraud, that is:

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; and

b. to knowingly and willfully devise and execute and attempt to execute, a scheme and artifice to defraud a financial institution, 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.

Objects of the Conspiracy

196. The objects of the conspiracy included:

a. using interstate and foreign wire transmissions to infect computers with Trickbot malware designed to capture victims' online banking credentials and other confidential personal and financial information;

b. using the captured banking credentials to pose as victims and gain access to victims' online bank accounts at financial institutions in the United States and elsewhere;

c. initiating unauthorized wire transfers of victim funds held in United States financial institutions; and

d. laundering stolen funds using United States and foreign beneficiary bank accounts controlled by the Trickbot Group.

Manner and Means of the Conspiracy

197. The manner and means used to accomplish the conspiracy are set forth in Paragraphs 76 – 95 of this Indictment and are re-alleged and incorporated by reference as if fully set forth herein.

198. To infect victims' computer with Trickbot malware, Defendants and other Trickbot 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 and installed Trickbot malware onto victims' computers without their knowledge or consent.

199. Once installed on the victim computer, Trickbot malware captured the victims' online banking login credentials and other confidential private and online banking information.

200. To fraudulently gain unauthorized access to victims' online bank accounts, Defendants and other Trickbot Conspirators, known and unknown to the Grand Jury, used the

victims' captured online banking login credentials without authorization to falsely represent to banks and financial institutions that Defendants and other Trickbot Conspirators were the victims, were authorized to access the victims' bank accounts, and were authorized to make electronic funds transfers from the victims' bank accounts.

Acts in Furtherance of the Conspiracy

201. In furtherance of the conspiracy and to effect the objects thereof, Defendants, and others known and unknown to the Grand Jury, committed the following acts, among others, in the Northern District of Ohio and elsewhere.

202. On or about the dates listed below, Defendants ANDREY ZHUYKOV, aka ZHUIKOV, aka DIF, aka DEF, aka DEFENDER; DMITRY PUTILIN, aka GRAD, aka STAFF; SERGEY LOGUNTSOV, aka BEGEMOT, aka ZULAS; MAX MIKHAYLOV, aka BAGET; MAKSIM RUDENSKY, aka FONIN, aka BINMAN; and MAKSIM KHALIULLIN, aka MAXFAX, aka MAXHAX, aka KAGAS and others known and unknown to the Grand Jury, for purposes of executing the above-described scheme and artifice, which scheme affected a financial institution, caused to be transmitted by means of wire communications in interstate and foreign commerce the writings, signs, signals, pictures and sounds described below:

	Approximate Date	Victim	Approximate Amount of Wire/ Attempted Wire Authorization	Originating Location	Destination Location
a.	October 19, 2017	CW 1	$98,177	Avon, OH	Buckeye Community Bank, Lenexa, MO
b.	October 19, 2017	CW 1	$98,373	Avon, OH	Buckeye Community Bank, Lenexa, MO
c.	October 19, 2017	CW 1	$175,789	Avon, OH	Buckeye Community Bank, Lenexa, MO

	Approximate Date	Victim	Approximate Amount of Wire/ Attempted Wire Authorization	Originating Location	Destination Location
d.	October 19, 2017	CW 1	$98,727	Avon, OH	Buckeye Community Bank, Lenexa, MO
e.	October 19, 2017	CW 1	Login to CW1 online banking account	Cleveland, OH	Buckeye Community Bank, Lenexa, MO
f.	October 20, 2017	CW 1	Login to CW1 online banking account and attempted wire transfer of $691,570	Lilburn, GA	Buckeye Community Bank, Lenexa, MO
g.	March 30, 2018	CW 5	$438,900	Key Bank Solon, OH	Turkiye Cumhuriyeti Ziraat Bankask, Ankara, Turkey
h.	March 30, 2018	CW 5	$171,299	Key Bank Solon, OH	Turkiye Cumhuriyeti Ziraat Bankask, Ankara, Turkey
i.	March 30, 2018	CW 5	$184,900	Key Bank Solon, OH	Bank of America New York, NY
j.	March 30, 2018	CW 5	$79,450	Key Bank Solon, OH	TD Bank, Mt. Laurel, NJ
k.	September 28, 2018	CW 8	$485,900	Regions Bank, Hoover, AL	Turkiye Cumhuriyeti Ziraat Bankask, Ankara, Turkey
l.	September 28, 2018	CW 8	$479,500	Regions Bank, Hoover, AL	Yapi Ve Kredi Bankasi A.S., Istanbul, Turkey
m.	September 28, 2018	CW 8	$398,900	Regions Bank, Hoover, AL	Denizbank A.S. Istanbul, Turkey
n.	September 28, 2018	CW 8	$398,900	Regions Bank, Hoover, AL	Turkiye Cumhuriyeti Ziraat Bankask, Ankara, Turkey
o.	September 28, 2018	CW 8	$395,400	Regions Bank, Hoover, AL	QNB Finansbank A.S., Istanbul, Turkey

	Approximate Date	Victim	Approximate Amount of Wire/ Attempted Wire Authorization	Originating Location	Destination Location
p.	October 3, 2018	CW 3	$230,400	Huntington National Bank, Columbus, OH	Bank of America New York, NY
q.	October 3, 2018	CW 3	$84,900	Huntington National Bank, Columbus, OH	Bank of America New York, NY
r.	October 3, 2018	CW 3	$154,200	Huntington National Bank, Columbus, OH	Bank of America New York, NY
s.	October 3, 2018	CW 3	$171,200	Huntington National Bank, Columbus, OH	Citibank New York, NY
t.	October 3, 2018	CW 3	$84,200	Huntington National Bank, Columbus, OH	Santander Bank, Wilmington, DE
u.	October 3, 2018	CW 3	$44,900	Huntington National Bank, Columbus, OH	HSBC, Buffalo, NY
v.	February 7, 2019	CW 11	$198,370	CoBank, Greenwood, CO	Fio Banka, A.S. Prague, Czechia
w.	February 7, 2019	CW 11	$73,411	CoBank, Greenwood, CO	Caixabank, S.A. Barcelona, Spain
x.	February 7, 2019	CW 11	$78,123	CoBank, Greenwood, CO	Caixabank, S.A. Barcelona, Spain
y.	February 7, 2019	CW 11	$170,212	CoBank, Greenwood, CO	Wells Fargo Bank San Francisco, CA

	Approximate Date	Victim	Approximate Amount of Wire/ Attempted Wire Authorization	Originating Location	Destination Location
z.	February 7, 2019	CW 11	$62,341	CoBank, Greenwood, CO	Nationwide Swindon, United Kingdom
aa.	February 7, 2019	CW 11	$98,663	CoBank, Greenwood, CO	Bank of America, New York, NY
bb.	February 7, 2019	CW 11	$183,941	CoBank, Greenwood, CO	Bank of America, New York, NY
cc.	February 7, 2019	CW 11	$193,112	CoBank, Greenwood, CO	Bank of America, New York, NY
dd.	February 7, 2019	CW 11	$194,312	CoBank, Greenwood, CO	Bank of America, New York, NY

203. On or about the dates listed below, Defendants ANDREY ZHUYKOV, aka ZHUIKOV, aka DIF, aka DEF, aka DEFENDER; DMITRY PUTILIN, aka GRAD, aka STAFF; SERGEY LOGUNTSOV, aka BEGEMOT, aka ZULAS; MAX MIKHAYLOV, aka BAGET; MAKSIM RUDENSKY, aka FONIN, aka BINMAN; and MAKSIM KHALIULLIN, aka MAXFAX, aka MAXHAX, aka KAGAS and others known and unknown to the Grand Jury, for purposes of executing the above-described scheme and artifice to defraud the financial institutions listed below and for obtaining money under the custody and control of said financial institutions, by means of false and fraudulent pretenses, representations and promises, obtained access to the online accounts and caused and attempted to cause fraudulent wire transfers as set forth below:

	Approximate Date(s)	Financial Institution	False Pretenses/ Representations
a.	December 12, 2016	U.S. Bank	Unauthorized use of CW 4's online banking credentials and wire transfer of approximately $44,000 from U.S. Bank.

	Approximate Date(s)	Financial Institution	False Pretenses/ Representations
b.	October 17, 2017 to October 19, 2017	Buckeye Community Bank	Unauthorized use of CW 1's online banking credentials and wire transfers of approximately $98,177; $98,373; $175,789; and $98,727 from Buckeye Community Bank.
c.	October 19, 2017 to October 20, 2017	Buckeye Community Bank	Unauthorized use of CW 1's online banking credentials and attempted wire transfer of approximately $691,570 from Buckeye Community Bank.
d.	March 30, 2018	Key Bank	Unauthorized use of CW 5's online banking credentials and wire transfers and attempted wire transfers of approximately $438,900; $171,299; $184,900; and $79,450 from Key Bank.
e.	May 16, 2018	People's United Bank	Unauthorized use of CW 6's online banking credentials and wire transfers and attempted wire transfers of approximately $1,250,000 and $50,000 from People's United Bank.
f.	September 28, 2018	First National Bank	Unauthorized use of CW 7's online banking credentials and wire transfers and attempted wire transfers of approximately $98,847 and $100,000 from First National Bank.
g.	October 3, 2018	First National Bank	Unauthorized use of CW 7's online banking credentials and attempted wire transfer of approximately $100,000 from First National Bank.
h.	September 28, 2018	Regions Bank	Unauthorized use of CW 8's online banking credentials and wire transfers and attempted wire transfers of approximately $485,900; $479,500; $398,900; $398,900 and $395,400 from Regions Bank.
i.	October 3, 2018	Huntington National Bank	Unauthorized use of CW 3's online banking credentials and wire transfers and attempted wire transfers of approximately $230,400; $84,900; $154,200; $171,200; $84,200, $44,900 and $89,400 from Huntington National Bank.
j.	December 10, 2018	J.P. Morgan Chase Bank	Unauthorized use of CW 10's online banking credentials and wire transfers and attempted wire transfers of approximately $800,000; $900,000; $890,000; and $950,000 from J.P. Morgan Chase Bank.

	Approximate Date(s)	Financial Institution	False Pretenses/ Representations
k.	February 7, 2019	CoBank	Unauthorized use of CW 11's online banking credentials and wire transfers and attempted wire transfers of approximately $198,370; $73,411; $78,123; $170,212; $62,341; $98,663; $183,941; $193,112; and $194,312 from CoBank.

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

COUNT 3
(Conspiracy to Commit Money Laundering, 18 U.S.C. § 1956(h))

The Grand Jury further charges:

204. The factual allegations of Paragraphs 1 – 72, 97 – 193, and 202 – 203 of this Indictment are hereby re-alleged and incorporated by reference as if fully set forth herein.

The Conspiracy

205. From in or around November 2015 through the date of this Indictment, in the Northern District of Ohio, Eastern Division and elsewhere, Defendants MIKHAIL TSAREV, aka MANGO; ANDREY ZHUYKOV, aka ZHUIKOV, aka DIF, aka DEF, aka DEFENDER; MAKSIM GALOCHKIN, aka BENTLEY; DMITRY PUTILIN, aka GRAD, aka STAFF; SERGEY LOGUNTSOV, aka BEGEMOT, aka ZULAS; MAX MIKHAYLOV, aka BAGET; MAKSIM RUDENSKY, aka FONIN, aka BINMAN; VALENTIN KARYAGIN, aka GLOBUS; and MAKSIM KHALIULLIN, aka MAXFAX, aka MAXHAX, aka KAGAS and others known and unknown to the Grand Jury, did knowingly and intentionally combine, conspire, confederate and agree with each other to commit offenses against the United States in violation of Title 18, United States Code, Section 1956, to wit:

a. to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, which transactions involved the proceeds of

specified unlawful activity, that is, Wire Fraud, in violation of Title 18, United States Code, Section 1343, Bank Fraud, in violation of Title 18, United States Code, Section 1344 and Fraudulent Access to Computers, in violation of Title 18, United States Code, Section 1030, knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership and control of the proceeds of specified unlawful activity and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i);

b. to transport, transmit and transfer and attempt to transport, transmit and transfer a monetary instrument and funds involving the proceeds of specified unlawful activity, that is, Wire Fraud, in violation of Title 18, United States Code, Section 1343, Bank Fraud, in violation of Title 18, United States Code, Section 1344 and Fraudulent Access to Computers, in violation of Title 18, United States Code, Section 1030, from a place in the United States to and through a place outside the United States, knowing that the funds involved in the transportation, transmission and transfer represented the proceeds of some form of unlawful activity and knowing that such transportation, transmission and transfer was designed in whole and in part to conceal and disguise the nature, location, source, ownership and control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(2)(B)(i); and

c. to knowingly engage and attempt to engage in a monetary transaction in criminally derived property with a value greater than $10,000, which property was derived from a specified unlawful activity, that is, Wire Fraud, in violation of Title 18, United States Code, Section 1343, Bank Fraud, in violation of Title 18, United States Code, Section 1344 and Fraudulent Access to Computers, in violation of Title 18, United States Code, Section 1030, by, through, and to a financial institution and affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1957.

Objects of the Conspiracy

206. The objects of the conspiracy included:

a. obscuring and disguising the ultimate recipients of the criminal proceeds of the Wire Fraud, Bank Fraud and Fraudulent Access to Computers schemes to defraud – as discussed above in Paragraphs 43 – 57, 76 – 95, 97 – 193, 198 – 200, and 202 – 203, by laundering those funds using a network of money mules and wire transfers conducted under the guise of legitimate businesses;

b. laundering those criminal proceeds through U.S. and foreign beneficiary bank accounts provided and controlled by Trickbot Conspirators; and

c. transferring money obtained from the Wire Fraud, Bank Fraud and Fraudulent Access to Computers schemes overseas for personal financial gain.

Manner and Means of the Conspiracy

207. The manner and means used to accomplish the conspiracy are set forth in Paragraphs 76 – 95 and 198 – 200 of this Indictment and are hereby re-alleged and incorporated by reference as if fully set forth herein.

208. Defendants and other Trickbot 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 the Trickbot Group.

209. The Trickbot Group advertised and posted listings for remote employment on job posting websites.

210. The Trickbot Group created fictitious companies, such as "Liberty Shopping" and "Element Construction Group," and created fraudulent websites for the companies to give the impression that they were actual businesses which engaged in legitimate domestic and international transactions.

211. The Trickbot Group explained to potential employees that they would be required to receive funds and distribute them to investors and vendors of the seemingly legitimate businesses.

212. The Trickbot Group instructed employees to open business banking accounts and further instructed the employees on how to provide answers to financial institutions in opening the business banking accounts.

213. The Trickbot Group would then send funds, consisting of criminal proceeds of Wire Fraud, Bank Fraud, and Fraudulent Access to Computers, to the employee's business banking account, either through ACH, wire transfer, or other electronic funds transfers, or through official check.

214. Shortly after the funds were deposited into the employee's business bank accounts, the Trickbot Group would instruct the employee to initiate an electronic funds transfer to an overseas financial account created by and under the control of the Trickbot Group.

Eventually these funds were transferred to members of the Trickbot Group for their personal enrichment.

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

ENHANCEMENT PURSUANT TO TITLE 18, UNITED STATES CODE, SECTION 3559(g)(1)
(False Registration of a Domain Name)

The Grand Jury further charges that:

215. The factual allegations of Paragraphs 1 – 72, 76 – 95, 97 – 193, 198 – 200, and 202 – 203 of this Indictment are hereby re-alleged and incorporated by reference as if fully set forth herein.

216. In furtherance of the offenses alleged in Counts 1 through 3, Defendants MIKHAIL TSAREV, aka MANGO; ANDREY ZHUYKOV, aka ZHUIKOV, aka DIF, aka DEF, aka DEFENDER; MAKSIM GALOCHKIN, aka BENTLEY; DMITRY PUTILIN, aka GRAD, aka STAFF; SERGEY LOGUNTSOV, aka BEGEMOT, aka ZULAS; MAX MIKHAYLOV, aka BAGET; MAKSIM RUDENSKY, aka FONIN, aka BINMAN; VALENTIN KARYAGIN, aka GLOBUS; and MAKSIM KHALIULLIN, aka MAXFAX, aka MAXHAX, aka KAGAS, together with others known and unknown to the Grand Jury, knowingly falsely registered and caused to be falsely registered, domain names and knowingly used and caused to be used said domain names in the course of committing the offenses alleged in Counts 1 through 2, namely, PUTILIN, together with others unknown to the Grand Jury, registered domains, including autoxrace.com, jabbb.biz, hzgit.biz, testinghostfortest.biz, hztest.biz, vboxdata.biz, bplace.biz, serverv.biz, campingtrue.biz, colibri-logistics-ltd.com, zidarkman16.com, zidarkman.com, gametester.pro, imperial-logistics.pro, jabong-online.com, yoox-online.com, boohoo-online.com, colette-online.com, coas2coast.com, busysnob.com, employje.com, resursvolkov.com,

srkpgfcbi.ru, cbutcjyrgjc.ru, gtgnmxsd.ru, fabwnebkxer.ru, forkosdavery.com, rqhgrmlmda.ru, baralianada.ru, grmdmbqvq.ru, idyjinmxcvy.ru, theinvoicefax.org, infodocuments.com, invoicefax.com, infodocuments.org, trustclub.biz, thetrio.biz, phoenix-logistics-llc.com, swallow-logistics-llc.com, gss-llc.com, smrtest-logistics-llc.com, zidarkman.biz, albatros-logistics.com, superadminz.com and testadmino.ru with false names and addresses in a manner that prevented the effective identification of and contact with Defendants and other Trickbot Conspirators and used those domains in the course of committing the felony offenses charged in Counts 1 through 3,

All in violation of Title 18, United States Code, Section 3559(g)(1).

FORFEITURE: COUNTS 1 - 2

The Grand Jury further charges:

217. The allegations contained in Counts 1-2 of this Indictment are hereby re-alleged and incorporated by reference as if fully set forth herein for the purpose of alleging forfeiture pursuant to the provisions of 18 U.S.C. §§ 982(a)(2)(A), 982(a)(2)(B) and 1030(i). As a result of these offenses, Defendants MIKHAIL TSAREV, aka MANGO; ANDREY ZHUYKOV, aka ZHUIKOV, aka DIF, aka DEF, aka DEFENDER; MAKSIM GALOCHKIN, aka BENTLEY; DMITRY PUTILIN, aka GRAD, aka STAFF; SERGEY LOGUNTSOV, aka BEGEMOT, aka ZULAS; MAX MIKHAYLOV, aka BAGET; MAKSIM RUDENSKY, aka FONIN, aka BINMAN; VALENTIN KARYAGIN, aka GLOBUS; and MAKSIM KHALIULLIN, aka MAXFAX, aka MAXHAX, aka KAGAS, shall forfeit to the United States: (i) any and all property constituting, or derived from, any proceeds they obtained, directly or indirectly, as the result of such offenses; and, (ii) any and all personal property that was used – or was intended to

be used – to commit or to facilitate the commission of the offense charged in Count 1 of the Indictment.

FORFEITURE: COUNT 3

The Grand Jury further charges:

218. The allegations contained in Count 3 of this Indictment are hereby re-alleged and incorporated by reference as if fully set forth herein for the purpose of alleging forfeiture pursuant to the provisions of 18 U.S.C. § 982(a)(1). As a result of this offense, Defendants MIKHAIL TSAREV, aka MANGO; ANDREY ZHUYKOV, aka ZHUIKOV, aka DIF, aka DEF, aka DEFENDER; MAKSIM GALOCHKIN, aka BENTLEY; DMITRY PUTILIN, aka GRAD, aka STAFF; SERGEY LOGUNTSOV, aka BEGEMOT, aka ZULAS; MAX MIKHAYLOV, aka BAGET; MAKSIM RUDENSKY, aka FONIN, aka BINMAN; VALENTIN KARYAGIN, aka GLOBUS; and MAKSIM KHALIULLIN, aka MAXFAX, aka MAXHAX, aka KAGAS, shall forfeit to the United States all property, real and personal, involved in such offense and all property traceable to such property.

A TRUE BILL.

Original document - Signatures on file with the Clerk of Courts, pursuant to the E-Government Act of 2002.

United States v. Mikhail Tsarev, et al.

A TRUE BILL.

_____
FOREPERSON

_____
REBECCA C. LUTZKO
United States Attorney