AO 442 (Rev. 11/11) Arrest Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Ohio

FILED BY JAO D.C.
Feb 8, 2021
ANGELA E. NOBLE
CLERK U.S. DIST. CT.
S. D. OF FLA. - Miami

United States of America
v.
ALLA WITTE, aka MAX

Defendant

Case No. 1:20 CR 440

1:21-2236-MJ-OTAZO-REYES

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay

(name of person to be arrested) ALLA WITTE, aka MAX,

who is accused of an offense or violation based on the following document filed with the court:

☑ Indictment ☐ Superseding Indictment ☐ Information ☐ Superseding Information ☐ Complaint

☐ Probation Violation Petition ☐ Supervised Release Violation Petition ☐ Violation Notice ☐ Order of the Court

This offense is briefly described as follows:

18 USC § 371 Conspiracy to Commit Computer Fraud and Aggravated Identity Theft
18 USC § 1349 Conspiracy to Commit Wire and Bank Fraud
18 USC § 1343 Wire Fraud
18 USC § 1344 Bank Fraud
18 USC § 1028A(a)(1) Aggravated Identity Theft
18 USC § 1956(h) Conspiracy to Commit Money Laundering

Date: 8/13/20

Issuing officer's signature

City and state: Cleveland, Ohio

Printed name and title

Return

This warrant was received on *(date)* 09-14-2020, and the person was arrested on *(date)* _____ at *(city and state)* _____.

Date: _____

Arresting officer's signature

Printed name and title

FILED
AUG 13 2020
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF OHIO
CLEVELAND

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

UNITED STATES OF AMERICA, Plaintiff, v. [redacted] ALLA WITTE, aka MAX, [redacted] Defendants.	INDICTMENT JUDGE OLIVER CASE NO. 1:20 CR 440 Title 18, United States Code, Sections 371, 1028A(a)(1), 1030, 1343, 1344, 1349, 1956(h) and 2

GENERAL ALLEGATIONS

At all times relevant to this Indictment:

1. Defendants [redacted] ALLA WITTE, aka MAX; [redacted] and others presently 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 Suriname.

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 allows 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 was usually done surreptitiously by a computer program (i.e., keylogger) to capture the keys typed on a computer without the typist's knowledge. Malware that used keystroke logging would often 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

---

[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 the Defendants.

then access the victim's online bank account and execute unauthorized electronic funds transfers (EFT), such as Automated Clearing House (ACH) payments or wire transfers,[2] to accounts that they controlled.

5. "HTTP" ("Hypertext Transfer Protocol") 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 when a user who is 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.

---

[2] EFT 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.

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 "botnet" was an interconnected network of computers infected with malware without the knowledge of the computers' users that was controlled by a remote party, often referred to as a "botherder," who does not have authorization to control the computers on the network.

10. A "bot" was one of the infected computers that was part of a botnet and controlled by a remote party who does not have authorization to control the computer. For purposes of this Indictment, all "bots" were infected computers, and all infected computers were bots.

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

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

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

14. A "worm" was a term used to describe 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. Two-Factor Authentication was a common security feature used by web-based services that stored confidential personal and online financial information, such as banks. Two-Factor Authentication required the use of two independent mechanisms to verify the authenticity and identity of the user. Examples of Two-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 access to a victim's computer and/or computer files until the payment of a ransom

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

18. A "Malware Manager" was a member of the scheme generally responsible for recruiting and hiring "Malware Developers" (as that term is defined below), procuring infrastructure, managing finances, testing malware against CAV services, and deploying and monitoring the malware.

19. 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.

20. "Phishing" was a criminal scheme in which the perpetrators used mass email messages and/or fake websites to trick people into providing information, such as network credentials (e.g., usernames and passwords), that could later be used to gain access to a victim's systems. Phishing schemes often used social engineering techniques similar to traditional con-artist techniques in order to trick victims into believing they were providing their information to a trusted vendor, customer, or other acquaintance. Phishing emails were also often 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 their knowledge or permission.

21. "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.

22. Social engineering was a skill developed over time by people who wanted to acquire protected information through manipulation of social relationships. People who were skilled in social engineering could convince individuals to divulge protected information or access credentials that the social engineer deemed valuable to the achievement of his or her aims.

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. "Counter Anti-Virus" (CAV) services checked malware against anti-virus software to determine if the malware would be detected by the anti-virus software. CAVs did

not share and distribute uploaded malware files with anti-virus companies, but instead provided anonymity to malware developers and users.

26. The following were financial institutions, within the meaning of Title 18, Section 20, United States Code, whose deposits were insured by the Federal Deposit Insurance Corporation (FDIC) (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.

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

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

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

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

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

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

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

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

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

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

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

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

39. Unless otherwise noted, all communications of Defendants and conspirators set forth in this Indictment were translated from Russian to English.

THE TRICKBOT SCHEME TO DEFRAUD

40. "Dyre" was an online banking trojan operated by unknown individuals based in Moscow, Russia, that began targeting non-Russian businesses and entities in mid-2014. In or around November 2015, Russian authorities purportedly 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."

41. From in or around November 2015 and continuing through the date of this Indictment, Defendants [redacted] ALLA WITTE, aka MAX; [redacted] and others presently known and unknown to the Grand Jury, were part of a transnational organized cybercrime network and 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, Mexico, Spain, and Russia, through the use of the Trickbot malware.

42. Specifically, the Defendants and others 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 the defendants and others; and (f) install ransomware on victim computers.

43. Members of the scheme were located in multiple countries around the world including, but not limited to, Russia, Belarus, Ukraine and Suriname.

44. In order to perpetrate their criminal schemes, the 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, operate, and deploy 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 the Defendants and others.

45. The 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.

46. The 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.

47. 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.

48. Trickbot infected millions of victim computers worldwide.

49. 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.

50. 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. The 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 the Defendants.

51. Trickbot began victimizing businesses, schools and individuals in the United States and elsewhere in the world in or around Fall 2016.

THE DEFENDANTS

52. Defendant, [redacted] was a national and citizen of Russia. [redacted] resided in [redacted] Russia, and used the online monikers [redacted] 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.

53. Defendant [redacted] was a national and citizen of Russia. During the timeframe of this Indictment, [redacted] resided in [redacted] Russia, and used the online monikers [redacted] was a Malware Manager and had roles and responsibilities in the Trickbot Group similar to [redacted]

54. Defendant [redacted] was a national and citizen of Russia. During the timeframe of the Indictment, [redacted] resided in [redacted] Russia, and used the online monikers [redacted] 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.

55. Defendant [redacted] was a citizen and national of Russia. During the timeframe of this Indictment, [redacted] resided in [redacted] Russia, and used the online moniker [redacted] was a Malware 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.

56. Defendant [redacted] was a citizen and national of Russia. During the timeframe of this indictment [redacted] resided in the [redacted] Russia and in [redacted] was a Malware Developer for the Trickbot Group, overseeing the creation of internet browser injection, machine identification, and data harvesting codes used by the Trickbot malware.

57. Defendant ALLA WITTE, aka MAX, was a national of Russia. During the timeframe of this indictment, 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 ransomware, obtaining payments from ransomware victims, and developing tools and protocols for the storage of credentials stolen and exfiltrated from victims infected by Trickbot.

58. Defendant [redacted] was a citizen and national of Ukraine. During the timeframe of this indictment [redacted] resided in [redacted] 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.

CO-CONSPIRATORS

59. Co-Conspirator 8 ("CC8") was a Malware Manager who outlined programming needs, managed finances and deployed Trickbot.

60. Co-Conspirators 9, 10, 11 and 12 ("CC9, CC10, CC11, CC12") were Malware Developers and computer programmers for Trickbot.

61. Co-Conspirator 13 ("CC13") was a Malware Developer who provided completed modules of Trickbot malware to [redacted] and others to be crypted.

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

63. 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:

64. Paragraphs 1 through 63 of this Indictment are hereby re-alleged and incorporated by reference as if fully set forth herein.

The Conspiracy

65. From in or around November 2015 through the date of this Indictment, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendants [redacted] ALLA WITTE, aka MAX; [redacted] and others presently 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 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(i);

b. to intentionally 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 dollars in a one-year period, in violation of 18 U.S.C. §§ 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 18 U.S.C. §§ 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 18 U.S.C. §§ 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 or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, in violation of 18 U.S.C. §§ 1030(a)(7)(C) and 1030(c)(3)(A); and

f. knowingly possessing, transferring and using, without lawful authority, a means of identification of another person, during and in relation to felony violations of 18 U.S.C. §§ 1030, 1343, and 1344, to wit, Computer Fraud, Wire Fraud and Bank Fraud, in violation of 18 U.S.C. § 1028A(a)(1).

Object of the Conspiracy

66. The objects of the conspiracy included for the Defendants 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 networked with the initial 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 conspirators; and

f. infect victims' computers with ransomware.

Manner and Means of the Conspiracy

It was part of the conspiracy that:

67. 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.

68. The Defendants 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.

69. The Defendants 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.

70. The Defendants 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 the Defendants.

71. The Defendants crypted Trickbot to evade detection by anti-virus software and other protective measures used by victims.

72. The Defendants 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.

73. The Defendants spread Trickbot through a campaign of spamming, phishing and spear phishing. The Defendants designed the emails used in these campaigns to falsely represent that they were from legitimate companies, associations or organizations.

74. The Defendants 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.

75. The Defendants designed Trickbot, once it infected a computer system, 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.

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

77. The Defendants used keystroke logging to steal victims' online banking credentials when the victims logged into their online bank account from their infected computer.

78. The Defendants also used web injects to display false online banking pages on the victim's web browser that captured online banking information as the victim entered it and then transmitted the captured data back to the Defendants.

79. To defeat multi-factor authentication and other protective means used by financial institutions to protect their clients, the Defendants monitored the internet activity of infected computers to determine when the victims visited a financial institution webpage. The Defendants then used captured confidential information of the victims and contacted the victims, posing as bank security personnel, to interact with victims and employees of victim businesses to deceive them into providing the Defendants with their multi-factor authentication codes.

80. The Defendants further designed Trickbot to automatically detect, harvest and exfiltrate credentials and passwords stored in internet browsers on victims' computers.

81. The Defendants used the confidential personal and financial information obtained by Trickbot to falsely represent to banks and financial institution that the Defendants and their co-conspirators were victims or employees of victims who had authorization to access the victims' bank accounts and to make electronic funds transfers from the victims' bank accounts.

82. The Defendants 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.

83. The Defendants then used money mules to receive the wire transfers, ACH payments and other electronic funds transfers from the victims' bank accounts.

84. The Defendants then directed and caused the money mules to further transfer the stolen funds to reach the control of other members of the conspiracy.

85. The Defendants later used Trickbot as a service for other criminal efforts, including the deployment and use of ransomware.

86. In order to achieve the objects of this conspiracy, the 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 stolen credit cards and false credentials 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. encrypting emails and attachments, and 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; and

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

Overt Acts

87. In furtherance of the conspiracy, and to effect the objects thereof, the 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 TO TRICKBOT GROUP

88. On or about November 11, 2015, [redacted] obtained credentials to a private server used by the operators of the Dyre malware. Approximately a week later, members of the Dyre malware campaign were purportedly arrested by Russian authorities. [redacted] and others transitioned their operation to the creation of a new malware based on the Dyre framework.

89. Beginning no later than on or about December 4, 2015, [redacted] 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, maintain and deploy the Trickbot malware.

B. ACQUIRING SERVERS, VPNS AND VPS SERVICES

90. Beginning no later than in or around June 2015 through in or around April 2019, [redacted] used a PayPal account under his control to purchase VPS and VPN 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 then later for the Trickbot Group.

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

92. On or about December 7, 2015, [redacted] 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
[redacted]	Everything got disrupted in one second
CC8	We are restoring everything bit by bit
[redacted]	Yes, it is hard work, but I am sure everything will be restored. Thank you again. I will do some work now.
	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

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

94. On or about December 9, 2015, [redacted] agreed with the co-conspirators that he would register each server under a different account and email and was offered over 100 different emails by a co-conspirator to achieve this goal.

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

---

[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.

96. Throughout 2016 [redacted] maintained a detailed record of server specifications, leases, and payments for servers he and other acquired for the development, maintenance and deployment of Trickbot.

97. Beginning in or around January 2016 [redacted] and [redacted] began discussing the need to acquire "fullz," or full identifiers including name, date of birth, social security number and other identifiers, of Americans to conduct fraud on banks.

98. On or about February 1, 2016, [redacted] and [redacted] 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."

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

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

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

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

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

103. In or around January 2016 [redacted] agreed to work for and join the Trickbot Group.

104. On or about February 29, 2016, [redacted] introduced [redacted] to CC8, a leader of the Trickbot Group, in order for [redacted] to begin recruiting computer programmers on behalf of the group.

105. On or about May 3, 2016, [redacted], CC8 and CC9 agreed to purchase fee-based access to Russian and Belarussian-based job websites to gain access to resumes for computer programmers looking for employment.

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

107. Beginning no later than in or around March 2016 the 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.

108. On or about May 4 and May 16, 2016, [redacted] created the Gmail accounts ishteryakovruslan@gmail.com and department.ishteryakov@gmail.com to create accounts on job-listing websites and to use these accounts to communicate with potential recruits to the Trickbot Group.

109. On or about May 4, 2016, [redacted] contacted CC9 to obtain an already-existing document showing an Individual Tax Number (ITN), the Russian equivalent of an Employee Identification Number, to use to obtain an account on the Russian-based job website.

110. On or about May 4, 2016, CC9 provided [redacted] with links to images of existing companies based in Moscow to use for registering on the job website.

111. On or about June 15, 2016, [redacted] provided CC9 with the access information for the department.ishteryakov@gmail.com account on a job-posting site.

112. On or about June 30, 2016, [redacted] and CC9 discussed the wording of a recruitment posting on the Russian-based job website. CC9 advised [redacted] to not 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 [redacted] to "go ahead" and post the job posting.

113. On or about July 8, 2016, [redacted] provided CC9 with the access information for the department.ishteryakov@gmail.com account on the Russian-based job-posting site.

114. On or about July 26, 2016, [redacted] told [redacted] 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."

115. On or about July 26, 2016, [redacted] responded to [redacted] 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. 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."

116. On or about July 7, 2016, CC9 instructed [redacted] 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 [redacted] to only talk directly to potential recruits about the injection code.

D. RECRUITMENT OF [redacted]

117. On or about May 17, 2016, [redacted] used the department.ishteryakov@gmail.com email account to contact [redacted] and separately sent [redacted] an email from the Russian-language job site to send [redacted] a test task for the Trickbot Group.

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

119. In or around July 2016 [redacted] applied for two additional positions with the Trickbot Group and received test tasks for both vacancies.

120. On or about July 19, 2016, [redacted] sent an email to the Trickbot Group at the department.ishteryakov@gmail.com email stating [redacted] was having problems with the test task. That same day, [redacted] provided [redacted] response to CC8.

121. On or about July 21, 2016, [redacted] completed the task and sent the response to the Trickbot Group at the department.ishteryakov@gmail.com email. In the email, [redacted] 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.

122. On or about July 25, 2016, [redacted] and CC8 discussed [redacted] application and completion of the test task. During the conversation, [redacted] and CC8 noted that their test tasks were considered "blackhat" hacking. The text of the conversation follows:

CC8	[redacted]
CC8	[redacted] did the test task
CC8	Who else did it?
CC8	Why are you communicating with this one
CC8	[redacted] wrote to you
CC8	The main reason is that this functionality can be used for illegal activities/ blackhat (formgrabbing, injects) \n I do not do Blackhat
CC8	plus, [redacted] did not even do the test task
[redacted]	Later [redacted] changed his mind and [redacted] is ready to write in the evening. There is nothing to lose if [redacted] writes, right?
	Is [redacted] 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
[redacted]	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
[redacted]	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
[redacted]	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, [redacted] 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	[redacted] is already doing a good job) there are a lot of people
CC8	We'll find several decent programmers

123. On or about July 25, 2016, [redacted] obtained credentials to a private Trickbot Group communications server.

E. RECRUITMENT OF [redacted]

124. On or about May 27, 2016 [redacted] used the department.ishteryakov@gmail.com email to contact [redacted] and present him with a test task for the Trickbot Group.

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

126. On or about May 30, 2016, [redacted] used the department.ishteryakov@gmail.com to ask [redacted] to complete a second task involving altering a Firefox browser.

---

[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.

127. On or about June 1, 2016, [redacted] completed the Firefox browser alteration and provided a Dropbox URL linked to the completed task to [redacted]

128. On or about June 2, 2016, [redacted] provided [redacted] Dropbox URL to "CC9." After CC9 reviewed the code, CC9 and [redacted] engaged in the following conversation concerning [redacted]:

CC9	It's all working.
CC9	It's all correct.
CC9	The guy did the job.
[redacted]	Fucking awesome.)
	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.
CC9	Just need to come to an agreement with CC8...
CC9	where we should put him.
[redacted]	Maybe write to him about Jabber for now?
CC9	No.
CC9	Nothing for now.
[redacted]	Well, and also tell CC12, so that he registers [him].

CC9	No.
[redacted]	Okay.
CC9	We'll manage it ourselves.
CC9	Just on pause for now.
[redacted]	But otherwise everything is fucking 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, [redacted] and CC9 continued the conversation as follows:

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

129. Following this conversation, [redacted] and CC9 provided [redacted] with credentials and information to join the Trickbot Group and its private communication server.

F. DEVELOPMENT OF THE TRICKBOT MALWARE

130. In or around January 2016 [redacted] obtained credentials for the Trickbot private server from his co-conspirators and began providing malware code to the Trickbot Group.

131. From no later than in or around February 2016 through the date of this Indictment [redacted] provided computer code and technical support used in the development and maintenance of the Trickbot malware, including code that allowed the Trickbot Group to manage and control infected victim bots and code that facilitated spamming campaigns meant to infect victim computers with Trickbot malware.

132. On or about July 26, 2016, shortly after [redacted] received credentials to the private Trickbot communications server, [redacted] provided a file called "injector/module.rtf" to the Trickbot Group. This file provided guidance to the Trickbot Group on how the malware would monitor the activity on infected computers and web inject into internet browser sessions.

133. On or about that same day, [redacted] provided a file to the Trickbot Group called "injector/inj.rtf", which provided instruction to the conspirators on how to configure the injection files in the Trickbot malware.

134. On or about July 27, 2016, [redacted] 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.

135. On or about and between July 28, 2016, and June 1, 2018, [redacted] 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.

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

137. On or about and between July 27, 2016, and the date of this Indictment, [redacted] 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.

138. On or about September 3, 2018, [redacted] 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.

139. On or about and between September 3, 2018, and the date of this Indictment, [redacted] 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.

140. On or about the dates listed below, [redacted] submitted and caused to be 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.

141. On or about and between February 24, 2017 and November 15, 2018, [redacted] 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.

142. On or about September 19, 2016, [redacted] communicated with a Trickbot co-conspirator regarding the provision of code needed for the Trickbot malware.

143. On or about Sept 26, 2016, [redacted] forwarded code used for the Trickbot malware to the Trickbot Group.

144. On or about and between September 27 and October 2, 2016, [redacted] 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.

145. On or about November 14, 2016, [redacted] 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 spoof banking websites controlled by the Trickbot Group.

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

147. On or about February 10, 2017, [redacted] 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.

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

149. No later than on or about December 11, 2017, [redacted] gained access to the Trickbot development server.

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

151. On or about March 10, 2018, the Trickbot Group registered an account with VirusCheckmate ("VCM"), another counter anti-virus checker that was advertised on well-known underground cybercriminal forums.

152. Between in or around March and October 2018, the Trickbot Group uploaded approximately over 43,000 files to VCM. Some of the files had names such as "HSBC_deposit_Confirmation-0", "paypal", and "Bankline_Secure_Message."

153. On or about April 3, 2018, [redacted] modified and provided a technical document concerning Trickbot's operation to the Trickbot Group.

154. On or about October 2, 2018, WITTE gained access to the Trickbot development server.

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

156. 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.

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

158. On or about and between August 19, 2019, and the date of this Indictment, [redacted] 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.

159. On or about and between October 2019 and the date of this Indictment, WITTE provided code to the Trickbot Group to operate and deploy the Trickbot ransomware module. This code included the following

a. A web panel used to operate the Trickbot ransomware module, which included panels for "targets," "bots" and "users" of the ransomware and contained code that automatically doubled ransom amounts if a victim did not pay within a time period determined by the Trickbot Group; and

b. A web page used to inform victims that their computer was encrypted with ransomware and to provide a Bitcoin address used by Trickbot Group to obtain a ransom payment. The web page included the following language: "Your computer has been infected! Your documents, photos, databases and other important filed encrypted. To decrypt your filed you need to buy our special software."

160. On or about and between September 30, 2019, and the date of this Indictment, WITTE provided code to the Trickbot Group for a web panel used to access victim data stored in a database. The database contained a large number of credit card numbers and stolen credentials from the Trickbot botnet. This database also included a repository of information about infected

machines available as bots. WITTE provided code to this repository that showed an infected computer or 'bot' status in different colors based on the colors of a traffic light and allowed other Trickbot Group members to know when their co-conspirators were working on a particular infected machine.

161. On or about January 14, 2020, WITTE conducted internet searches for "laravel faker bitcoin address," a reference to creating a fake Bitcoin address to use to test the ransomware payment system.

162. On or about the dates listed below, [redacted] provided, modified and updated malware code for the Trickbot Group as follows, each modification or update consisting of a separate overt act:

Dates	Description of Code
July 2016 – Present	Modifications of Firefox Internet Browser
December 2016	Machine Query that allows Trickbot to determine the description, manufacturer, name, product, serial number, version and root file directory contents of an infected machine
August 2016 – December 2018	Grabs and saves browser name, ID, type, configuration files, (HTTP) cookies, history, local storage, & Flash Local Shared Objects/LSO (Flash cookies) from internet browsers.
October 2016 – Present	Searches for, imports and loads files present in internet browser's "profile" folders including cookies, storage, history, and Flash LSO cookies; also creates a connection to the browsers' databases to make queries, deletions and insertions.
July 2016 – Present	An executable app/utility used to launch & manage a browser.
July 2016 – present	Harvesting and modifying data entries stored in Google's (Chrome) LevelDB database, including browsing history.

II. DEPLOYMENT OF TRICKBOT

163. Beginning no later than October 2016 the Trickbot Group, from a location outside the United States, purchased and configured C2 servers that hosted malware and spam

campaigns and were used to host web inject servers for spoofed bank websites, and began deploying Trickbot malware to victims throughout the world.

164. No later than on or about January 31, 2017, [redacted] created and obtained a document entitled "спам", which was Russian for "Spam." Within the document were detailed instructions for [redacted] to:

a. First obtain Trickbot malware from CC13;

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.

165. Trickbot 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 their computers, each 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 and Bank Fraud, 18 U.S.C. § 1349)

The Grand Jury further charges:

166. The factual allegations of Paragraphs 1–63 and 88–165 of this Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth herein.

167. From in or around November 2015 continuing through the date of this Indictment, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendants [redacted] ALLA WITTE, aka MAX; and [redacted] and others presently known and unknown to the Grand Jury did knowingly and intentionally combine, conspire, confederate and agree with others 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

168. 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

169. The manner and means used to accomplish the conspiracy are set forth in Paragraphs 67 through 86 of this Indictment and are repeated, re-alleged and incorporated by reference as if fully set forth herein.

170. In order to infect victims' computer with Trickbot malware, the Defendants and conspirators known and unknown to the Grand Jury crafted and transmitted through the internet in interstate and foreign commerce phishing emails containing malicious hyperlinks or

attachments which, when clicked, downloaded and installed Trickbot malware onto victims' computers without their knowledge or consent.

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

172. In order to fraudulently gain unauthorized access to victims' online bank accounts, the Defendants, and conspirators known and unknown to the Grand Jury, used the victims' captured online banking login credentials without authorization to falsely represent to banks that the Defendants and their conspirators were victims or employees of victims who had authorization to access the bank accounts and to make electronic funds transfers from said accounts.

Acts in Furtherance of the Conspiracy

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

174. On or about the dates listed below, Defendants [redacted] ALLA WITTE, aka MAX; [redacted] and others, 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.	10/19/2017	CW 1	$98,177	Avon, OH	Buckeye Community Bank, Lenexa, MO
b.	10/19/2017	CW 1	$98,373	Avon, OH	Buckeye Community Bank, Lenexa, MO
c.	10/19/2017	CW 1	$175,789	Avon, OH	Buckeye Community Bank, Lenexa, MO
d.	10/19/2017	CW 1	$98,727	Avon, OH	Buckeye Community Bank, Lenexa, MO
e.	10/19/2017	CW 1	Login to CW1 online banking account	Cleveland, OH	Buckeye Community Bank, Lenexa, MO
f.	10/20/2017	CW 1	Login to CW1 online banking account and attempted wire transfer of $691,570	Lilburn, GA	Buckeye Community Bank, Lenexa, MO
g.	3/30/2018	CW 5	$438,900	Key Bank Solon, OH	Turkiye Cumhuriyeti Ziraat Bankask, Ankara, Turkey
h.	3/30/2018	CW 5	$171,299	Key Bank Solon, OH	Turkiye Cumhuriyeti Ziraat Bankask, Ankara, Turkey
i.	3/30/2018	CW 5	$184,900	Key Bank Solon, OH	Bank of America New York, NY
j.	3/30/2018	CW 5	$79,450	Key Bank Solon, OH	TD Bank, Mt. Laurel, NJ
k.	9/28/2018	CW 8	$485,900	Regions Bank, Hoover, AL	Turkiye Cumhuriyeti Ziraat Bankask, Ankara, Turkey
l.	9/28/2018	CW 8	$479,500	Regions Bank, Hoover, AL	Yapi Ve Kredi Bankasi A.S., Istanbul, Turkey

	Approximate Date	Victim	Approximate Amount of Wire/ Attempted Wire Authorization	Originating Location	Destination Location
m.	9/28/2018	CW 8	$398,900	Regions Bank, Hoover, AL	Denizbank A.S. Istanbul, Turkey
n.	9/28/2018	CW 8	$398,900	Regions Bank, Hoover, AL	Turkiye Cumhuriyeti Ziraat Bankask, Ankara, Turkey
o.	9/28/2018	CW 8	$395,400	Regions Bank, Hoover, AL	QNB Finansbank A.S., Istanbul, Turkey
p.	10/3/2018	CW 3	$230,400	Huntington National Bank, Columbus, OH	Bank of America New York, NY
q.	10/3/2018	CW 3	$84,900	Huntington National Bank, Columbus, OH	Bank of America New York, NY
r.	10/3/2018	CW 3	$154,200	Huntington National Bank, Columbus, OH	Bank of America New York, NY
s.	10/3/2018	CW 3	$171,200	Huntington National Bank, Columbus, OH	Citibank New York, NY
t.	10/3/2018	CW 3	$84,200	Huntington National Bank, Columbus, OH	Santander Bank, Wilmington, DE
u.	10/3/2018	CW 3	$44,900	Huntington National Bank, Columbus, OH	HSBC, Buffalo, NY
v.	2/07/2019	CW 11	$198,370	CoBank, Greenwood, CO	Fio Banka, A.S. Prague, Czechia
w.	2/07/2019	CW 11	$73,411	CoBank, Greenwood, CO	Caixabank, S.A. Barcelona, Spain
x.	2/07/2019	CW 11	$78,123	CoBank, Greenwood, CO	Caixabank, S.A. Barcelona, Spain
y.	2/07/2019	CW 11	$170,212	CoBank, Greenwood, CO	Wells Fargo Bank San Francisco, CA
z.	2/07/2019	CW 11	$62,341	CoBank, Greenwood, CO	Nationwide Swindon, United Kingdom

	Approximate Date	Victim	Approximate Amount of Wire/ Attempted Wire Authorization	Originating Location	Destination Location
aa.	2/07/2019	CW 11	$98,663	CoBank, Greenwood, CO	Bank of America, New York, NY
bb.	2/07/2019	CW 11	$183,941	CoBank, Greenwood, CO	Bank of America, New York, NY
cc.	2/07/2019	CW 11	$193,112	CoBank, Greenwood, CO	Bank of America, New York, NY
dd.	2/07/2019	CW 11	$194,312	CoBank, Greenwood, CO	Bank of America, New York, NY

175. On or about the dates listed below, Defendants [redacted] ALLA WITTE, aka MAX; [redacted] and others, 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.	12/12/2016	U.S. Bank	Unauthorized use of CW 4's online banking credentials and wire transfer of approximately $44,000 from U.S. Bank.
b.	10/17/2017 to 10/19/2017	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.

	Approximate Date(s)	Financial Institution	False Pretenses/ Representations
c.	10/19/2017 to 10/-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.	3/30/2018	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.	5/16/2018	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.	9/28/2018	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.	10/3/2018	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.	9/28/2018	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.	10/3/2018	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.	12/10/2018	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.	2/07/2019	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.

COUNTS 3 – 11
(Wire Fraud, 18 U.S.C. § 1343)

The Grand Jury further charges:

176. The factual allegations of Paragraphs 1 – 63, 88 – 165, and 174 – 175 of this Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth herein.

177. From in or around November 2015 continuing through the date of this Indictment, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendants [redacted] ALLA WITTE, aka MAX; and [redacted] and others presently known and unknown to the Grand Jury devised a scheme and artifice to defraud victims of the Trickbot malware and to obtain money and property, which scheme affected a financial institution, by means of false and fraudulent pretenses, representations and promises, as described above in Paragraphs 40 – 51, 67 – 86, 88 – 165, 170 – 172, and 174 – 175.

178. On or about the dates listed below, for purposes of executing and attempting to execute the above-described scheme and artifice to defraud and to obtain money and property,

which scheme affected a financial institution, Defendants [redacted] ALLA WITTE, aka MAX; [redacted] and others sent and caused to be sent by means of wire communications in interstate and foreign commerce the writings, signs, signals, pictures and sounds described below:

Count	Defendants	Approximate Date	Description of Wire	Originating Location	Recipient Location
3	[redacted]	10/19/2017	Login and Authorization for $98,177	Avon, OH	Buckeye Community Bank, Lenexa, MO
4		10/19/2017	Login and Authorization for $98,373	Avon, OH	Buckeye Community Bank, Lenexa, MO
5		10/19/2017	Login and Authorization for $175,789	Avon, OH	Buckeye Community Bank, Lenexa, MO
6		10/19/2017	Login and Authorization for $98,727	Avon, OH	Buckeye Community Bank, Lenexa, MO
7		10/19/2017	Login to CW1 online banking account	Cleveland, OH	Buckeye Community Bank, Lenexa, MO
8		3/30/2018	Approximate $438,900 wire transfer from CW 5's bank account	Key Bank Solon, OH	Turkiye Cumhuriyeti Ziraat Bankask, Ankara, Turkey

Count	Defendants	Approximate Date	Description of Wire	Originating Location	Recipient Location
9	[redacted]	3/30/2018	Approximate attempted $171,299 wire transfer from CW 5's bank account	Key Bank Solon, OH	Turkiye Cumhuriyeti Ziraat Bankask, Ankara, Turkey
10	[redacted]	3/30/2018	Approximate $184,900 wire transfer from CW 5's bank account	Key Bank Solon, OH	Bank of America New York, NY
11	[redacted]	3/30/2018	Approximate $79,450 wire transfer from CW 5's bank account	Key Bank Solon, OH	TD Bank, Mt. Laurel, NJ

All in violation of Title 18, United States Code, Section 1343 and 2.

COUNTS 12 – 31
(Bank Fraud, 18 U.S.C. § 1344)

The Grand Jury further charges:

179. The factual allegations of Paragraphs 1 – 63, 88 – 165, and 174 – 175 of this Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth here.

180. From in or around November 2015 continuing through the date of this Indictment, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendants [redacted] ALLA WITTE, aka MAX; and [redacted] and others presently known and unknown to the Grand Jury having devised and intended to devise a scheme and artifice to defraud a financial institution, as

that term is defined in Title 18, United States Code, Section 20 and listed below, and to obtain monies and funds in the custody and control of the below financial institutions by means of material false and fraudulent pretenses, representations and promises, namely, the scheme and artifice described above in Paragraphs 40 – 51, 67 – 86, 88 – 165, 170 – 172, and 174 – 175 of this Indictment, well knowing at the time that the pretenses, representations and promises would be and were false and fraudulent when made, did knowingly execute and attempt to execute the foregoing scheme and artifice by gaining access to online bank accounts and causing, and attempting to cause, the transfer of funds, with each access, transfer and attempted transfer being a separate count as set forth below:

Count	Defendants	Approximate Date	Financial Institution	Description
12	[redacted]	10/17/2017	Buckeye Community Bank, Lorain, OH	Login for CW 1's Online Banking Account
13		10/19/2017	Buckeye Community Bank, Lorain, OH	Approximate $98,177 wire transfer from CW 1's bank account
14		10/19/2017	Buckeye Community Bank, Lorain, OH	Approximate $98,373 wire transfer from CW 1's bank account
15		10/19/2017	Buckeye Community Bank, Lorain, OH	Approximate $175,789 wire transfer from CW 1's bank account
16		10/19/2017	Buckeye Community Bank, Lorain, OH	Approximate $98,727 wire transfer from CW 1's bank account

Count	Defendants	Approximate Date	Financial Institution	Description
17	[redacted]	10/19/2017	Buckeye Community Bank, Lorain, OH	Login for CW 1's Online Banking Account
18	[redacted]	10/20/2017	Buckeye Community Bank, Lorain, OH	Approximate $691,570 attempted wire transfer from CW 1's bank account
19	[redacted]	3/30/2018	Key Bank, Solon, OH	Login for CW 5's Online Bank Account
20	[redacted]	3/30/2018	Key Bank, Solon, OH	Approximate $438,900 wire transfer from CW 5's bank account
21	[redacted]	3/30/2018	Key Bank, Solon, OH	Approximate attempted $171,299 wire transfer from CW 5's bank account
22	[redacted]	3/30/2018	Key Bank, Solon, OH	Approximate $184,900 wire transfer from CW 5's bank account
23	[redacted]	3/30/2018	Key Bank, Solon, OH	Approximate $79,450 wire transfer from CW 5's bank account

Count	Defendants	Approximate Date	Financial Institution	Description
24	[redacted] WITTE [redacted]	10/03/2018	Huntington National Bank, North Canton, OH	Login for CW 3's Online Banking Account
25	[redacted] WITTE [redacted]	10/03/2018	Huntington National Bank, North Canton, OH	Approximate $230,400 wire transfer from CW 3's bank account
26	[redacted] WITTE [redacted]	10/03/2018	Huntington National Bank, North Canton, OH	Approximate $84,900 wire transfer from CW 3's bank account
27	[redacted] WITTE [redacted]	10/03/2018	Huntington National Bank, North Canton, OH	Approximate $154,200 wire transfer from CW 3's bank account
28	[redacted] WITTE [redacted]	10/03/2018	Huntington National Bank, North Canton, OH	Approximate $171,200 wire transfer from CW 3's bank account
29	[redacted] WITTE [redacted]	10/03/2018	Huntington National Bank, North Canton, OH	Approximate $84,200 wire transfer from CW 3's bank account

Count	Defendants	Approximate Date	Financial Institution	Description
30	[redacted] WITTE	10/03/2018	Huntington National Bank, North Canton, OH	Approximate $44,900 wire transfer from CW 3's bank account
31	[redacted] WITTE [redacted]	10/03/2018	Huntington National Bank, North Canton, OH	Approximate $89,400 wire transfer from CW 3's bank account

All in violation of Title 18, United States Code, Section 1344 and 2.

COUNTS 32 – 46
(Aggravated Identity Theft, 18 U.S.C. §§ 1028A(a)(1) and 2)

The Grand Jury further charges:

181. The factual allegations of Paragraphs 1 – 63, 67 – 86, 88 – 165, 170 – 172, and 174 – 175 of this Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth herein.

182. The term "means of identification," for purposes of this Indictment, means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual and includes any name, social security number, date of birth, and unique electronic identification code, address or routing code, including a credit or debit card number or an online banking credential and password.

183. On the dates noted below, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendants [redacted]

[redacted] ALLA WITTE, aka MAX; [redacted] and others presently known and unknown to the Grand Jury, did knowingly use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in 18 U.S.C. §1028A(c), to wit, the felony commission of Computer Fraud, a violation of Title 18, United States Code, Section 1030, Wire Fraud, a violation of Title 18, United States Code, Section 1343, and Bank Fraud, a violation of Title 18, United States Code, Section 1344, knowing that the means of identification belonged to another actual person:

Count	Defendants	Victim	Location	Approximate Dates of Theft and Use
32	[redacted]	K.H.	Avon, OH	10/17/2017 Online Bank Account Access
33		K.H.	Avon, OH	10/17/2017 to 10/19/2017 Approximate $98,177 wire transfer
34		K.H.	Avon, OH	10/17/2017 to 10/19/2017 Approximate $98,373 wire transfer
35		K.H.	Avon, OH	10/17/2017 to 10/19/2017 Approximate $175,789 wire transfer
36		K.H.	Avon, OH	10/17/2017 to 10/19/2017 Approximate $98,727 wire transfer

Count	Defendants	Victim	Location	Approximate Dates of Theft and Use
37	[redacted]	K.H.	Avon, OH	10/19/2017 Online Bank Account Access
38	[redacted]	K.H.	Avon, OH	10/19/2017 to 10/20/2017 Approximate $691,570,000 attempted wire transfer
39	[redacted] WITTE	J.A., L.M.	North Canton, OH	10/03/2018 Online Bank Account Access
40	[redacted] WITTE	J.A., L.M.	North Canton, OH	10/03/2018 Approximate $230,400 wire transfer
41	[redacted] WITTE	J.A., L.M.	North Canton, OH	10/03/2018 Approximate $84,900 wire transfer
42	[redacted] WITTE [redacted]	J.A., L.M.	North Canton, OH	10/03/2018 Approximate $154,200 wire transfer

Count	Defendants	Victim	Location	Approximate Dates of Theft and Use
43	[redacted] WITTE	J.A., L.M.	North Canton, OH	10/03/2018 Approximate $171,200 wire transfer
44	[redacted] WITTE	J.A., L.M.	North Canton, OH	10/03/2018 Approximate $84,200 wire transfer
45	[redacted] WITTE	J.A., L.M.	North Canton, OH	10/03/2018 Approximate $44,900 wire transfer
46	[redacted] WITTE [redacted]	J.A., L.M.	North Canton, OH	10/03/2018 Approximate $89,400 wire transfer

184. Members of the Trickbot Group knew, and had reason to know, that the information collected was from actual individuals because the means by which it was collected was specifically designed to require response and affirmative action by the victim to provide his or her own verification information.

185. Moreover, members of the Trickbot Group knew, and had reason to know, the online banking information was from actual individuals because the members successfully used the online banking credentials to gain access to online banking accounts and initiate and attempt to initiate wire transfers of funds.

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

COUNT 47
(Conspiracy to Commit Money Laundering, 18 U.S.C. § 1956(h))

The Grand Jury further charges:

186. The factual allegations of Paragraphs 1 – 63, 88 – 165, and 174 – 175 of this Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth herein.

The Conspiracy

187. From in or around November 2015 through the date of this Indictment, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendants [redacted] ALLA WITTE, aka MAX; [redacted] and others presently known and unknown to the Grand Jury, did knowingly and intentionally combine, conspire, and agree with each other and with other persons known and unknown to the Grand Jury 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 18 U.S.C.

§ 1343, Bank Fraud, in violation of 18 U.S.C. § 1344, and Fraudulent Access to Computers, in violation of 18 U.S.C. § 1030, knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of 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 or funds involving the proceeds of specified unlawful activity, that is, Wire Fraud, in violation of 18 U.S.C. § 1343, Bank Fraud, in violation of 18 U.S.C. § 1344, and Fraudulent Access to Computers, in violation of 18 U.S.C. § 1030, from a place in the United States to or 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 or 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 18 U.S.C. § 1343, Bank Fraud, in violation of 18 U.S.C. § 1344, and Fraudulent Access to Computers, in violation of 18 U.S.C. § 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

188. The objects of the conspiracy included for the Defendants to:

a. obscure and disguise 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 40 – 51, 67 – 86, 88 – 165, 170 – 172, and 174 – 175 – by laundering launder those funds using a network of money mules and wire transfers conducted under the guise of legitimate businesses;

b. launder those criminal proceeds through U.S. and foreign beneficiary bank accounts provided and controlled by conspirators; and

c. transfer 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

189. The manner and means used to accomplish the conspiracy are set forth in Paragraphs 67 – 86 and 170 – 172 of this Indictment and are repeated, re-alleged and incorporated by reference as if fully set forth herein.

190. The Defendants, and co-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.

191. The Trickbot Group advertised and posted listings for remote employment on job posting websites such as Indeed.com, LinkedIn.com and others.

192. 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.

193. 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.

194. 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.

195. 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.

196. 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).

FORFEITURE: COUNTS 1 - 31

The Grand Jury further charges:

197. The allegations contained in Counts 1-31 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 Title 18, United States Code, Section 982(a)(2) and Title 18, United States Code, Section 1030(i). As a result of these offenses, Defendants [redacted] ALLA WITTE, aka MAX; [redacted] 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 47

The Grand Jury further charges:

198. The allegations contained in Count 47 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 Title 18, United States Code, Section 982(a)(1). As a result of this offense, Defendants [redacted] ALLA WITTE, aka MAX; [redacted] 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. [redacted] et. al.

A TRUE BILL.

FOREPERSON

JUSTIN E. HERDMAN
United States Attorney