UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

March 2022 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

v.

ALEKSANDR STEPANOV,
aka "JimmBee,"
aka "Clay Barton,"
aka "Monster,"
DANIL KHALITOV,
aka "Flawless,"
aka "Dancho,"
FNU LNU,
aka "Pin_Plus,"
aka "Pin,"
ALEKSEY EFREMOV,
aka "Ahost,"
KAMIL SZTURGULEWSKI,
aka "RaZZputin,"
aka "bank666,"
aka "kgb666,"
IBRAHIM IDOWU,
aka "daveedo,"
aka "audrops,"
aka "sostransfer,"
aka "Ronald 22,"
aka "Ronshop,"
ARTEM SHUBIN,
aka "Krad,"
ALEKSEY KHUDYAKOV,
aka "Bshayne,"
aka "Moddixpb,"
aka "BarboSpidor,"

CR LACR22-0429-FLA

I N D I C T M E N T

[18 U.S.C. § 371: Conspiracy; 18 U.S.C. § 1349: Conspiracy to Commit Wire Fraud and Bank Fraud; 18 U.S.C. § 1028A: Aggravated Identity Theft; 18 U.S.C. § 1030(a)(2)(c), (c)(2)(B)(i), (c)(2)(B)(ii): Unauthorized Access to a Protected Computer to Obtain Information; 18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(VI): Unauthorized Impairment of a Protected Computer; 18 U.S.C. § 2511(1)(a) (Intercepting a Communication (Wiretapping)); 18 U.S.C. § 2511(1)(d) (Use of an Intercepted Communication); 18 U.S.C. §§ 981(a)(1)(C), 982, 1030, 28 U.S.C. § 2461(c): Criminal Forfeiture]

FNU LNU,
aka "Format,"
FNU LNU,
aka "Goldcoin,"
FNU LNU,
aka "Matrix8,"
FNU LNU,
aka "Hir0,"
FNU LNU,
aka "Chopin,"
FNU LNU,
aka "Benzz,"
FNU LNU,
aka "Linup,"

Defendants.

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS AND DEFINITIONS

At all times relevant to this Indictment:

1. DanaBot was a malicious software, or "malware." One of its main functions was to steal data, including information associated with online accounts, such as bank accounts, email accounts, social media accounts, e-commerce accounts, and cryptocurrency wallets, thereby enabling DanaBot users and other malicious actors to commit fraud, including by using victim credentials, such as victims' usernames and passwords, to drain monies from financial accounts. The malware was also designed to steal information such as credit card numbers, cryptocurrency wallet addresses, passwords, detailed computer system information, computer cookies, computer browsing history, and other data that could be used for fraud or sold to others for such use.

2. DanaBot had the ability to hijack victim banking sessions by injecting code or commands, known as "web injects," into victims' web sessions unbeknownst to victims, thereby allowing the malware to capture information or gain access to victims' online bank accounts,

or to redirect funds to accounts or payees not intended by victims. The malware could prevent a victim from visiting a particular website by redirecting the victim to a different website designed to appear to be the website the victim intended to visit. In this way, malicious actors could redirect victims to fraudulent sites, and, for example, prompt victims to enter their usernames and passwords.

3. DanaBot contained a keylogger that could be configured to track victims' keystrokes and thereby capture information such as file passwords, cryptocurrency passwords, and other credentials. DanaBot's keylogger could capture keystrokes that might be obfuscated on a screen, such as a hidden password.

4. DanaBot was designed to record videos of victim activity on the screens of compromised devices, such as when a victim was visiting a cryptocurrency website, operating a cryptocurrency wallet, or using a cryptocurrency application, thereby enabling theft of funds from a victim's cryptocurrency wallet(s).

5. DanaBot contained a remote access function, providing malicious actors full control over a victim's desktop and the ability to establish an Internet connection to a victim's computer so that the malicious actors could access the Internet from the victim computer's Internet Protocol ("IP") address. Known as "backconnect," this feature permitted various types of fraud by allowing malicious actors to pose as their victim and use the victim's assigned IP address while engaging in criminal activities over the Internet.

6. DanaBot was advertised on Russian-language criminal forums, including the forum Exploit.in ("Exploit"). In posts on the Exploit forum, DanaBot's developers described the features of their malware, including its ability to evade detection by many antivirus programs,

and invited collaborators and prospective customers to contact them using encrypted communication protocols to purchase the malware or to work with them on further development.

7. DanaBot could be purchased with different available modules, such as a version that included ransomware, and could be configured for other purposes, such as using infected computers to conduct distributed denial of service ("DDoS") attacks.

8. The DanaBot malware was available in two variants. The first variant (the "Criminal Variant") was used to target victims worldwide to engage in a variety of fraudulent activity. The central members of the DanaBot organization set up servers to transfer stolen victim data and information to servers from which malicious-actor-customers of the Criminal Variant could access and exploit the data.

9. The second variant (the "Espionage Variant") was used to target military, diplomatic, government, and non-governmental organizations. For this variant, separate servers were established, such that data stolen from these victims was ultimately stored in the Russian Federation ("Russia"). Unlike the Criminal Variant, the Espionage Variant was configured so that all victim interactions with a computer were video-recorded by default.

10. DanaBot's Criminal Variant was sold to a number of malicious actors known as "affiliates," or subscribers, who paid a monthly fee in order to use the malware and its associated software interface, described by the group as the "client." The client allowed affiliates to interact with the malware and review data stolen by the malware or interact directly with victims' computers. Each affiliate was assigned a particular number. In some cases, affiliates were assigned more than one number and, in some cases, an

affiliate number represented a group of criminal customers who targeted their fraudulent schemes at specific geographic areas. The affiliate numbers were encoded into the DanaBot malware and also used as a form of login credential.

11. Affiliates caused the DanaBot malware to be installed on victim computers via a variety of methods, including via "phishing" emails that falsely represented themselves to be legitimate emails from government entities, companies, associations, and organizations.

12. DanaBot's Criminal Variant infected over 300,000 computers, in almost every country in the world, with particular concentrations in the United States, Australia, Poland, India, and Italy. DanaBot also infected computers in numerous judicial districts within the United States, including many victim computers in the Central District of California.

13. The Espionage Variant infected computers in several countries, including the United States, Belarus, the United Kingdom, Germany, and Russia.

14. The DanaBot developers were located in Russia. DanaBot's affiliates were predominantly located in Russia but were also located in several other countries, including Poland and Thailand.

15. The U.S. financial institutions referenced herein that were targets of DanaBot-related fraud were insured by the Federal Deposit Insurance Corporation.

COUNT ONE

[18 U.S.C. § 371]

The Grand Jury hereby realleges and incorporates by reference paragraphs 1 through 15 of the Introductory Allegations and Definitions of this Indictment as though fully set forth herein.

A. OBJECTS OF THE CONSPIRACY

Beginning on an unknown date but prior to September 19, 2015, and continuing to on or about the date of this Indictment, in Los Angeles County, within the Central District of California, and elsewhere, defendants ALEKSANDR STEPANOV, also known as ("aka") "JimBee," aka "Clay Barton," aka "Monster" ("STEPANOV"); DANIL KHALITOV, aka "Flawless," aka "Dancho" ("KHALITOV"); FNU LNU, aka "Pin_Plus," aka "Pin" ("PIN PLUS"); ALEKSEY EFREMOV, aka "Ahost" ("EFREMOV"); KAMIL SZTURGULEWSKI, aka "RaZZputin," aka "bank666," aka "kgb666" (SZTURGULEWSKI); IBRAHIM IDOWU, aka "daveedo," aka "audrops," aka "sostransfer," aka "Ronald 22," aka "Ronshop" ("IDOWU"); ARTEM SHUBIN, aka "Krad" ("SHUBIN"); ALEKSEY KHUDYAKOV, aka "Bshayne," aka "Moddixpb," aka "BarboSpidor" ("KHUDYAKOV"); FNU LNU, aka "Format" ("FORMAT"); FNU LNU, aka "Goldcoin" ("GOLDCOIN"); FNU LNU, aka "Matrix8" ("MATRIX8"); FNU LNU, aka "Hir0" ("HIR0"); FNU LNU, aka "Chopin" ("CHOPIN"); FNU LNU, aka "Benzz" ("BENZZ"); and FNU LNU, aka "Linup" ("LINUP"); and others known and unknown to the Grand Jury, knowingly conspired and agreed with each other to:

1. intentionally access computers without authorization and thereby obtain information from protected computers, (a) for commercial advantage and private financial gain, and (b) in furtherance of criminal and tortious acts, in violation of Title 18, United States Code, Section 1030(a)(2)(C), (c)(2)(B)(i), (ii);

2. knowingly and with intent to defraud access protected computers without authorization, and by means of such conduct, further the intended fraud and obtain a thing of value, in violation of Title 18, United States Code, Section 1030(a)(4), (c)(3)(A);

3. knowingly cause the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally cause damage without authorization to protected computers, and specifically to cause (a) loss aggregating at least $5,000 in value during a one-year period, and (b) damage affecting ten or more protected computers during a one-year period, in violation of Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I), (c)(4)(A)(i)(VI);

4. intentionally intercept, endeavor to intercept, procure another person to intercept, and procure another person to endeavor to intercept electronic communications, in violation of Title 18, United States Code, Section 2511(1)(a); and

5. intentionally use and endeavor to use the contents of an electronic communication, knowing and having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1), in violation of Title 18, United States Code, Section 2511(1)(d).

B. MEANS BY WHICH THE OBJECTS OF THE CONSPIRACY WERE TO BE ACCOMPLISHED

The objects of the conspiracy were to be accomplished in substance as follows:

1. Defendant STEPANOV and an unindicted co-conspirator ("UICC No. 1") would work with other co-conspirators to create and develop the malware that came to be known as DanaBot.

2. Defendant STEPANOV and UICC No. 1 would advertise the DanaBot malware on Russian-language criminal forums, describing its functionality and its ability to evade detection by various antivirus programs.

3. Defendant STEPANOV and UICC No. 1 would sell subscriptions to, or lease, the DanaBot malware to affiliates. These subscriptions cost approximately $3,000 to $4,000 per month. Each affiliate would be assigned an affiliate number to use in accessing the DanaBot malware and the data it would steal.

4. Defendant STEPANOV, UICC No. 1, and other co-conspirators would provide a software-based control panel, the "client," for every affiliate. The client provided a method to view all of the data stolen from an affiliate's victims, as well as the ability to issue further commands to the victim computers, such as to download additional files, to search for specific terms on a victim's computer, to capture screenshots or videos, to turn on keylogging, and otherwise to control or access the victim computer or data stored therein.

5. UICC No. 1 and other co-conspirators would provide ongoing customer support to DanaBot affiliates in their use of the malware.

6. Defendant LINUP would perform technical tasks as assigned by UICC No. 1 relating to the DanaBot malware and servers used to administer the malware, such as how information would be displayed within the DanaBot client.

7. Defendant PIN PLUS would procure servers to support the operation of the Criminal Variant. These servers included web-inject servers, which maliciously redirected victim banking sessions to facilitate the theft of banking credentials and the draining of bank

accounts, and command-and-control servers, where data stolen from the victims would be routed and stored for later access by co-conspirators, and from which co-conspirators could issue commands to victim computers.

8. Defendant EFREMOV would obtain and provide use of such servers to defendant PIN PLUS, knowing that the servers were used for controlling the DanaBot botnet.

9. Defendants KHALITOV, PIN PLUS, SZTURGULEWSKI, IDOWU, SHUBIN, KHUDYAKOV, FORMAT, GOLDCOIN, MATRIX8, HIRO, CHOPIN, and BENZZ and other co-conspirators would purchase subscriptions, or work with affiliates who had purchased subscriptions, to use the DanaBot malware for a monthly fee.

10. Defendants KHALITOV, PIN PLUS, SZTURGULEWSKI, IDOWU, SHUBIN, KHUDYAKOV, FORMAT, GOLDCOIN, MATRIX8, HIRO, and BENZZ and other co-conspirators would use various means to infect victims with the DanaBot malware, including by sending campaigns of spam "phishing" email messages to thousands of recipients to get them to unwittingly install the malware. The phishing emails were designed to fraudulently entice victim recipients to click on a hyperlink or attachment that falsely represented itself to be a legitimate link or attachment, and often appeared to come from government or public entities. When the victim clicked on the link or attachment, the DanaBot malware, or an associated loader, would be downloaded onto the victim's computer without the victim's knowledge or consent.

11. Defendants KHALITOV, PIN PLUS, SZTURGULEWSKI, IDOWU, SHUBIN, KHUDYAKOV, FORMAT, GOLDCOIN, MATRIX8, HIRO, CHOPIN, and BENZZ and other co-conspirators would then use DanaBot malware to obtain the victims' data, including credentials, financial and

cryptocurrency account information, videos of the victims' use of the computers, victims' browsing and searching history, keystrokes, and other data deemed useful by the co-conspirators.

12. Defendants PIN PLUS, IDOWU, MATRIX8, HIRO, and BENZZ and other co-conspirators would use the web-inject capabilities of the DanaBot malware to intercept internet sessions of victim computers and obtain information provided by victims during such sessions.

13. Defendants KHALITOV, PIN PLUS, SZTURGULEWSKI, IDOWU, SHUBIN, KHUDYAKOV, FORMAT, GOLDCOIN, MATRIX8, HIRO, and BENZZ and other co-conspirators would use or attempt to use information stolen from the victims' computers and internet sessions to fraudulently obtain money from the victims' financial institutions or other payment services, including, in some cases, from United States banks insured by the Federal Deposit Insurance Corporation.

14. Defendant SZTURGULEWSKI and other co-conspirators would use the malware to install files containing Automatic Transfer System ("ATS") scripts, which would enable the co-conspirators to steal funds from victims' bank accounts, including by fraudulently redirecting transfers to accounts controlled by defendant SZTURGULEWSKI and other co-conspirators.

15. Defendant KHALITOV and other co-conspirators would use information obtained via the DanaBot malware to engage in fraudulent product-return schemes, which targeted the victims' retail operations and used victim credentials to authorize refunds for fraudulent purchases at high volumes.

16. Defendant KHALITOV and other co-conspirators would use stolen victim data to engage in various additional frauds, including using victim credentials to steal money from balances victims

maintained with online service providers, such as advertisers, payroll services, or ecommerce websites.

17. Defendants PIN PLUS, IDOWU, HIRO, and other co-conspirators would specifically target victims in Australia and New Zealand and would (1) use data stolen via the DanaBot malware to drain victim bank accounts and (2) inject traffic into victims' banking transactions in order to obtain credentials or redirect funds to the co-conspirators. Through this conduct, this group caused millions of dollars in losses to their victims and the victims' banks.

18. Defendants PIN PLUS, IDOWU, HIRO, and other co-conspirators would compromise corporate email servers in Australia and New Zealand, changing server rules to cause all incoming and outgoing email to be sent to the co-conspirators; in this way, they would obtain information that allowed them to commit additional fraudulent activity.

19. Defendant STEPANOV and UICC No. 1 and other co-conspirators would develop additional modules for the DanaBot malware, including a module that would allow a user to conduct DDoS attacks on other computers, and a module that would download ransomware to victim computers.

20. Unindicted co-conspirators would use the DanaBot malware to launch DDoS attacks on websites relating to the government of Ukraine, shortly after it had been invaded by Russia.

21. Defendant STEPANOV, UICC No. 1, and other co-conspirators would create the Espionage Variant of DanaBot and provide it to co-conspirators for use in targeting military, diplomatic, or non-governmental organization computers for infection.

22. Defendant STEPANOV and UICC No. 1, or another co-

conspirator, would set up separate servers and communication architecture for the Espionage Variant, by which stolen data would be transmitted to Russia.

23. Unindicted co-conspirators would use the Espionage Variant to compromise computers around the world and steal sensitive diplomatic communications, credentials, and other data from these targeted victims. This stolen data included financial transactions by diplomatic staff, correspondence concerning day-to-day diplomatic activity, as well as summaries of a particular country's interactions with the United States.

C. OVERT ACTS

On or about the following dates, in furtherance of the conspiracy and to accomplish its objects, defendants STEPANOV, KHALITOV, PIN PLUS, EFREMOV, SZTURGULEWSKI, IDOWU, SHUBIN, KHUDYAKOV, FORMAT, GOLDCOIN, MATRIX8, HIRO, CHOPIN, BENZZ, and LINUP, and others, committed various overt acts within the Central District of California and elsewhere, including, but not limited to, the following:

Overt Act No. 1: On September 19, 2015, defendant STEPANOV posted a message on the Russian-language online criminal forum Exploit, seeking investors or partners interested in working with him on a multipurpose malicious software.

Overt Act No. 2: On September 20, 2015, defendant STEPANOV posted a second message on Exploit describing the attributes of the malware as including a "form grabber" (i.e., a type of malware that grabs data from a webform, such as log-in credentials), a keylogger, and an injector.

Overt Act No. 3: On April 16, 2018, defendant STEPANOV posted

a message on Exploit describing the functionality of the malware he and other co-conspirators had been developing (which later became known as DanaBot), including the computer systems it would run on, its ability to remain invisible to the computers it infected, its inclusion of a keylogger, its ability to record video of the victim's screen and to perform various other operations, as well as descriptions of the server and client modules available to customers.

Overt Act No. 4: On April 17, 2018, defendant STEPANOV posted a message on Exploit indicating that the malware had been detected by only three out of 23 different antivirus programs.

Overt Act No. 5: On April 18, 2018, defendant STEPANOV posted a message on Exploit indicating that his malware had been detected by only six out of 23 different antivirus programs.

Overt Act No. 6: On April 18, 2018, defendant STEPANOV posted a message on Exploit saying that he believed he could bypass three more antivirus programs with a new technique.

Overt Act No. 7: On April 23, 2018, defendant STEPANOV posted a message on Exploit saying that he would not work with people who could not speak Russian, nor with people who did not have reputations.

Overt Act No. 8: On May 27, 2018, defendant STEPANOV posted a message on Exploit saying that he and other co-conspirators had improved several facets of the malware, and that they were ready to hire one or two more partners.

Overt Act No. 9: On May 28, 2018, defendant PIN PLUS installed DanaBot malware on a computer under his control.

Overt Act No. 10: On June 13, 2018, defendant STEPANOV posted a message on Exploit saying that the anonymous network Tor was

supported for restoring proxy servers for the malicious software, and one more partner was required for their team. He also stated that he and other co-conspirators needed someone to handle cryptocurrency-related schemes.

Overt Act No. 11: On September 11, 2018, an unindicted co-conspirator posted a message on Exploit saying that they had been using the malware for several weeks, and all of the features functioned properly. They also noted that the developers provided good support service, that the software was the best the unindicted co-conspirator had ever used, and all that was needed was a good way to get the malware onto victim computers.

Overt Act No. 12: On or about September 19, 2018, defendant SHUBIN, as DanaBot Affiliate No. 2, installed the DanaBot malware on a computer under his control.

Overt Act No. 13: In October 2018, defendant SZTURGULEWSKI and an unindicted co-conspirator purchased a subscription to the DanaBot malware for $3500 per month in Bitcoin from UICC No. 1 via the Exploit forum.

Overt Act No. 14: On October 16, 2018, after being notified that defendant PIN PLUS was using defendant EFREMOV's servers to control the DanaBot botnet, defendant EFREMOV continued to lease additional servers to defendant PIN PLUS.

Overt Act No. 15: On November 28, 2018, defendant PIN PLUS caused a victim computer to be infected with the DanaBot malware, resulting in the theft of that victim's banking information.

Overt Act No. 16: On December 7, 2018, UICC No. 1 made a video depicting his access to various DanaBot modules, while logged into the client software as "user-21."

Overt Act No. 17: On December 14, 2018, UICC No. 1 took a screenshot depicting his login to the DanaBot client software as "user-21."

Overt Act No. 18: On January 26, 2019, UICC No. 1 infected a computer under his control with the DanaBot malware.

Overt Act No. 19: On January 25, 2019, defendant SHUBIN caused a victim computer in Los Angeles, California, to be infected with the DanaBot malware.

Overt Act No. 20: On January 31, 2019, defendant KHUDYAKOV operated the DanaBot client, logging in as "User-9," at which time the client software indicated that defendant KHUDYAKOV had infected 463 victims with the DanaBot malware, with the most infections in Iran, Turkey, and Romania.

Overt Act No. 21: On February 8, 2019, defendant KHUDYAKOV used the DanaBot client application to view a list of DanaBot Affiliate No. 9's active DanaBot victims in Great Britain.

Overt Act No. 22: On February 8, 2019, defendant KHALITOV, as DanaBot Affiliate No. 10, installed the DanaBot malware on a computer under his control.

Overt Act No. 23: On February 12, 2019, defendant KHUDYAKOV, as DanaBot Affiliate No. 9, installed DanaBot malware on a computer under his control.

Overt Act No. 24: On February 19, 2019, defendant KHUDYAKOV contacted UICC No. 1 via a secure communication platform and asked about the status of the DanaBot botnet.

Overt Act No. 25: On February 19, 2019, UICC No. 1 told defendant KHUDYAKOV via a secure communication platform that the DanaBot servers and database had suffered a "glitch" but that the

problem had been solved.

Overt Act No. 26: On February 19, 2019, defendant KHUDYAKOV told UICC No. 1 via a secure communication platform that defendant KHUDYAKOV was having problems setting up loaders and bots and asked UICC No. 1 for an update on the matter.

Overt Act No. 27: On February 19, 2019, UICC No. 1 told defendant KHUDYAKOV via a secure communication platform that UICC No. 1 was assigned as "chief of support" and would look into the problem.

Overt Act No. 28: On February 19, 2019, defendant KHUDYAKOV told UICC No. 1 via a secure communication platform that he was "user-9."

Overt Act No. 29: On February 20, 2019, defendant PIN PLUS contacted UICC No. 1 via a secure messaging platform to discuss the status of the botnet and noted that the malware was being detected by Windows Defender.

Overt Act No. 30: On February 21, 2019, UICC No. 1 drafted a document containing a description of the DanaBot malware to be provided to customers, including how it worked and on what platforms, how it was controlled and accessed, what support was provided, and the various functionalities of the malware.

Overt Act No. 31: On February 26, 2019, defendant STEPANOV posted a message on Exploit saying that he and the other co-conspirators were still looking for additional partners.

Overt Act No. 32: On March 14, 2019, defendant STEPANOV, as DanaBot Affiliate No. 1, infected two computers under his control with the DanaBot malware.

Overt Act No. 33: On March 17, 2019, UICC No. 1 posted a message on Exploit answering a prospective customer's questions about

the malicious software, including about various build options and the effect of using a third-party crypting service.

Overt Act No. 34: On March 24, 2019, UICC No. 1 took a screenshot depicting his login to the DanaBot client software as the user "root."

Overt Act No. 35: On March 25, 2019, UICC No. 1, defendant CHOPIN and an unindicted co-conspirator communicated using a secure messaging platform regarding complications with encrypting and obfuscating the DanaBot malware.

Overt Act No. 36: On April 2, 2019, defendant SHUBIN, as DanaBot Affiliate No. 2, installed DanaBot malware on a computer under his control.

Overt Act No. 37: On April 5, 2019, UICC No. 1 posted a message on Exploit stating that the account listed for support was temporarily unavailable and that customers should contact him via a different account.

Overt Act No. 38: On April 6, 2019, defendant STEPANOV posted a message on Exploit saying that the DanaBot malware could now support additional file formats and that he and the other co-conspirators were seeking partners.

Overt Act No. 39: On May 5, 2019, defendants MATRIX8 and BENZZ worked with UICC No. 1 to establish a web-inject server targeting DanaBot victims communicating with U.S. financial institutions.

Overt Act No. 40: On May 11, 2019, defendant EFREMOV provided a server to defendant PIN PLUS, which was used to monitor, intercept, and potentially modify victim traffic with specific Australian financial institutions.

Overt Act No. 41: On May 11, 2019, defendant EFREMOV provided

another server to defendant PIN PLUS, which was used as a DanaBot "stage 1" backend, passing commands to victim computers and receiving data stolen from the victims before transmitting the data further to the backend storage server.

Overt Act No. 42: On May 13, 2019, UICC No. 1 posted a message on Exploit stating that all of the contact accounts were available and the co-conspirators were open for business.

Overt Act No. 43: On May 17, 2019, defendant IDOWU, as part of the DanaBot Affiliate No. 5 group, infected a computer under his control with DanaBot malware.

Overt Act No. 44: On May 18, 2019, defendant IDOWU searched for the term "Australia DL" [Driver's License] on the online criminal forum crdclub.cc.

Overt Act No. 45: On June 1, 2019, defendant IDOWU searched the criminal website "richlogs" for Facebook credentials for users located in Australia.

Overt Act No. 46: On June 12, 2019, defendant KHALITOV caused a victim computer in Los Angeles, California to be infected with the DanaBot malware.

Overt Act No. 47: On June 26, 2019, in response to a potential customer's request regarding the price and capabilities of the DanaBot malware, UICC No. 1 posted a message on Exploit instructing the potential customer to contact him via the secure messaging account provided in the signature of the posts.

Overt Act No. 48: On July 10, 2019, UICC No. 1 posted a message on Exploit stating that the DanaBot malware had been updated to include additional functionality.

Overt Act No. 49: In August 2019, UICC No. 1 exchanged

messages with a person he believed to be a potential customer, but who was in fact a confidential source working with the FBI, in which UICC No. 1 detailed the capabilities of the DanaBot malware and provided a document containing a written description of its functionality and instructions for new customers on how to use it.

Overt Act No. 50: In August 2019, defendant KHALITOV used login credentials obtained from DanaBot infections to initiate a fraudulent purchase and refund scheme on an e-commerce platform, in which KHALITOV stole over one million dollars from the victims and the e-commerce platform.

Overt Act No. 51: On September 10, 2019, defendant PIN PLUS notified UICC No. 1 via a secure messaging platform that he had provided a third party with two proxy servers.

Overt Act No. 52: On September 11, 2019, defendant UICC No. 1 created a document containing a list of file-download links for the DanaBot client application, instructional manual, and instructional video, as well as a list of affiliate IDs and their assignments.

Overt Act No. 53: On September 16, 2019, UICC No. 1 sent a message to defendant LINUP containing credentials for an Australia-based DanaBot victim, instructing defendant LINUP to make corrections related to a set of records and specifically noting that the DanaBot malware appeared to not collect passwords from the Firefox or Edge browsers, but that it worked properly in terms of stealing passwords from the Chrome browser.

Overt Act No. 54: On September 19, 2019, defendant KHALITOV caused a victim computer in Los Angeles, California to become infected with DanaBot malware.

Overt Act No. 55: On September 21, 2019, defendant KHALITOV

obtained the name, address, phone number, and full credit card number of a victim in Los Angeles, California, whose computer was infected with DanaBot malware.

Overt Act No. 56: On September 29, 2019, via a secure communication platform, UICC No. 1 instructed defendant LINUP to make certain changes to the DanaBot client relating to how various fields were displayed.

Overt Act No. 57: On September 29, 2019, via a secure communication platform, defendant LINUP responded to UICC No. 1 that he could make the changes in 10 to 15 minutes.

Overt Act No. 58: On October 9, 2019, defendant KHUDYAKOV transmitted an email message which contained a JavaScript downloader for the DanaBot malware.

Overt Act No. 59: On October 16, 2019, a co-conspirator infected a computer with DanaBot malware and then stole credentials for the [redacted] Police Department, including the username and password for several employees of the [redacted] Police Department.

Overt Act No. 60: On October 16, 2019, UICC No. 1 told a co-conspirator via a mobile-chat application that he had uploaded data relating to the [redacted] Police Department.

Overt Act No. 61: On December 30, 2019, UICC No. 1 uploaded a copy of the DanaBot client application to an online storage location.

Overt Act No. 62: On January 19, 2020, defendant STEPANOV posted a message on Exploit saying that he and other co-conspirators were looking for partners.

Overt Act No. 63: On January 21, 2020, defendant SZTURGULEWSKI repeatedly attempted to contact UICC No. 1.

Overt Act No. 64: On January 22, 2020, defendant SZTURGULEWSKI

ran the client file for the DanaBot malware on his computer.

Overt Act No. 65: On February 4, 2020, defendant KHALITOV, as DanaBot Affiliate No. 10, obtained information related to a 2019 United States tax filing from a computer infected with DanaBot.

Overt Act No. 66: On March 30, 2020, defendant FORMAT posted a message on Exploit saying that he recommended working with the DanaBot team, and noted certain issues that they were working on.

Overt Act No. 67: On April 28, 2020, UICC No. 1 posted a message on Exploit stating that most modules of the DanaBot malware had been updated and a few slots for additional customers had been added. UICC No. 1 also provided additional information about features of the DanaBot malware and other tools he and other co-conspirators had available to use with the DanaBot malware.

Overt Act No. 68: On March 16, 2020, defendant SZTURGULEWSKI possessed data stolen from users infected with the DanaBot malware on a computer at his home.

Overt Act No. 69: On February 10, 2021, UICC No. 1 created a document containing the email addresses of diplomatic representatives of many governments, several of whose computers had been infected with the DanaBot malware Espionage Variant.

Overt Act No. 70: On March 7, 2022, defendant STEPANOV posted a new advertisement on the Exploit forum for the DanaBot malware, titled "[For rent] DanaTools." The advertisement offered "Banking trojan DanaBot" in the following forms: "Basic kit" with a $500 one-time server install fee and a "Stealer" for $2000 per month; an "Advanced kit" with a "PostGrabber + Inject" for $1000 per month and an "Online Module" for $1000 per month; a "Full kit + installation" for $4,000 per month; and an "Extended kit" to be negotiated on a

case-by-case basis with additional capabilities. The advertisement further described the DanaBot malware's capabilities, including that it could do the following: record videos, processes, and websites; log keystrokes; intercept clipboard content; steal data entered into websites by a victim; conduct web injects; redirect web requests; block web requests; provide notification via Jabber of particular events or processes; steal files (in particular, wallets); steal data from browsers, other clients, and email programs; view a victim computer's screen, obtain command access to the victim's system, and have access to the victim's processes; provide a hidden desktop; and restore proxies via Tor. The advertisement also provided additional information about working with the malware and included a link to a demonstration video. Defendant STEPANOV stated that he and other co-conspirators were ready to provide a limited number of "slots" to customers and directed interested parties to contact UICC No. 1, and to contact defendant STEPANOV with other interesting cooperation offers.

Overt Act No. 71: On March 22, 2022, one or more co-conspirators used the DanaBot malware to launch DDoS attacks at websites used by government entities of Ukraine.

Overt Act No. 72: On March 26, 2022, defendant PIN PLUS commented on defendant STEPANOV's Exploit post, noting that it was "Clever professional software for various purposes," and adding, "my recommendations."

Overt Act No. 73: On May 11, 2022, defendant STEPANOV added a post to his thread on Exploit, saying that he and other co-conspirators had "added a mini bootloader from memory," and that they

were "preparing for the release of [a] Professional KIT" with "One or two spots...available."

Overt Act No. 74: On May 29, 2022, defendant STEPANOV responded to a post on Exploit asking if a DanaBot license could be purchased jointly with another Exploit user by saying that he and other co-conspirators only provided the malware, and it was up the buyer to determine how many trusted or authorized people or employees they needed.

Overt Act No. 75: On July 1, 2022, defendant STEPANOV added to his thread on Exploit, saying that there were spaces for partners, and also that spots were open to test the "professional kit."

Overt Act No. 76: On September 6, 2022, an unindicted co-conspirator posted a message on defendant STEPANOV's Exploit thread, saying that they had obtained a license for the DanaBot malware, the actors working on the software were good, the malware's components worked, and "the stealer robs what is needed," adding, "In a word, super."

COUNT TWO

[18 U.S.C. § 1349]

The Grand Jury hereby realleges and incorporates by reference paragraphs 1 through 15 of the Introductory Allegations and Definitions of this Indictment as though fully set forth herein.

A. OBJECTS OF THE CONSPIRACY

Beginning on an unknown date but prior to September 19, 2015, and continuing to on or about the date of this Indictment, in Los Angeles County, within the Central District of California, and elsewhere, defendants ALEKSANDR STEPANOV, also known as ("aka") "JimBee," aka "Clay Barton," aka "Monster" ("STEPANOV"); DANIL KHALITOV, aka "Flawless," aka "Dancho" ("KHALITOV"); FNU LNU, aka "Pin_Plus," aka "Pin" ("PIN PLUS"); ALEKSEY EFREMOV, aka "Ahost" ("EFREMOV"); KAMIL SZTURGULEWSKI, aka "RaZZputin," aka "bank666," aka "kgb666" (SZTURGULEWSKI); IBRAHIM IDOWU, aka "daveedo," aka "audrops," aka "sostransfer," aka "Ronald 22," aka "Ronshop" ("IDOWU"); ARTEM SHUBIN, aka "Krad" ("SHUBIN"); ALEKSEY KHUDYAKOV, aka "Bshayne," aka "Moddixpb," aka "BarboSpidor" ("KHUDYAKOV"); FNU LNU, aka "Format" ("FORMAT"); FNU LNU, aka "Goldcoin" ("GOLDCOIN"); FNU LNU, aka "Matrix8" ("MATRIX8"); FNU LNU, aka "Hir0" ("HIR0"); FNU LNU, aka "Chopin" ("CHOPIN"); FNU LNU, aka "Benzz" ("BENZZ"); FNU LNU, aka "Linup" ("LINUP"); and others known and unknown to the Grand Jury, knowingly conspired and agreed with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

B. MEANS BY WHICH THE OBJECTS OF THE CONSPIRACY WERE TO BE ACCOMPLISHED

The Grand Jury hereby repeats and realleges the Means by Which the Objects of the Conspiracy Were to be Accomplished set forth in

Section B of Count One of this Indictment as if fully set forth herein.

C. OVERT ACTS

The Grand Jury hereby repeats and realleges the Overt Acts set forth in Section C of Count One of this Indictment as if fully set forth herein.

COUNT THREE

[18 U.S.C. § 1028A]

Beginning on an unknown date but at least as early as August 2018, and continuing to on or about the date of this Indictment, in Los Angeles County, within the Central District of California, and elsewhere, defendants ALEKSANDR STEPANOV, also known as ("aka") "JimBee," aka "Clay Barton," aka "Monster" ("STEPANOV"); DANIL KHALITOV, aka "Flawless," aka "Dancho" ("KHALITOV"); FNU LNU, aka "Pin_Plus," aka "Pin" ("PIN PLUS"); ALEKSEY EFREMOV, aka "Ahost" ("EFREMOV"); KAMIL SZTURGULEWSKI, aka "RaZZputin," aka "bank666," aka "kgb666" (SZTURGULEWSKI); IBRAHIM IDOWU, aka "daveedo," aka "audrops," aka "sostransfer," aka "Ronald 22," aka "Ronshop" ("IDOWU"); ARTEM SHUBIN, aka "Krad" ("SHUBIN"); ALEKSEY KHUDYAKOV, aka "Bshayne," aka "Moddixpb," aka "BarboSpidor" ("KHUDYAKOV"); FNU LNU, aka "Format" ("FORMAT"); FNU LNU, aka "Goldcoin" ("GOLDCOIN"); FNU LNU, aka "Matrix8" ("MATRIX8"); FNU LNU, aka "Hir0" ("HIR0"); FNU LNU, aka "Chopin" ("CHOPIN"); FNU LNU, aka "Benzz" ("BENZZ"); and FNU LNU, aka "Linup" ("LINUP") knowingly transferred, possessed, and used, without lawful authority, means of identification that defendants STEPANOV, KHALITOV, PIN PLUS, EFREMOV, SZTURGULEWSKI, IDOWU, SHUBIN, KHUDYAKOV, FORMAT, GOLDCOIN, MATRIX8, HIR0, CHOPIN, BENZZ, and LINUP knew belonged to other persons, during and in relation to the offense of Conspiracy to Commit Wire Fraud, a felony violation of Title 18, United States Code, Section 1349, as charged in Count Two of this Indictment.

COUNT FOUR

[18 U.S.C. § 1349]

The Grand Jury hereby realleges and incorporates by reference paragraphs 1 through 15 of the Introductory Allegations and Definitions of this Indictment as though fully set forth herein.

A. OBJECTS OF THE CONSPIRACY

Beginning on an unknown date but prior to September 19, 2015, and continuing to on or about the date of this Indictment, in Los Angeles County, within the Central District of California, and elsewhere, defendants ALEKSANDR STEPANOV, also known as ("aka") "Clay Barton," "JimBee," and "Monster"; FNU LNU, aka "Matrix8"; and FNU LNU, aka "Benzz"; and others known and unknown to the Grand Jury, knowingly conspired and agreed with each other to commit bank fraud, in violation of Title 18, United States Code, Section 1344(2).

B. MEANS BY WHICH THE OBJECTS OF THE CONSPIRACY WERE TO BE ACCOMPLISHED

The Grand Jury hereby repeats and realleges the Means by Which the Objects of the Conspiracy Were to be Accomplished set forth in Section B of Count One of this Indictment as if fully set forth herein.

C. OVERT ACTS

The Grand Jury hereby repeats and realleges the Overt Acts set forth in Section C of Count One of this Indictment as if fully set forth herein.

COUNT FIVE

[18 U.S.C. § 1030(a)(2)(C), (c)(2)(B)(i), (c)(2)(B)(ii)]

Between or about February 2019 and September 2020, in Los Angeles County, within the Central District of California, and elsewhere, defendants ALEKSANDR STEPANOV, also known as ("aka") "JimBee," aka "Clay Barton," aka "Monster," and DANIL KHALITOV, aka "Flawless," aka "Dancho," intentionally accessed computers without authorization and thereby obtained information from protected computers, as that term is defined in Title 18, United States Code, Section 1030(e)(2)(B), for the purpose of private financial gain and in furtherance of a criminal act, to wit, Wire Fraud, in violation of Title 18, United States Code, Section 1343, and Use of an Unlawfully Intercepted Communication, in violation of Title 18, United States Code, Section 2511(d).

COUNT SIX

[18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(VI)]

Between or about February 2019 and September 2020, in Los Angeles County, within the Central District of California, and elsewhere, defendants ALEKSANDR STEPANOV, also known as ("aka") "JimBee," aka "Clay Barton," aka "Monster," and DANIL KHALITOV, aka "Flawless," aka "Dancho," knowingly caused the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally and without authorization caused damage by impairing the integrity and availability of data, programs, systems, and information on protected computers, as that term is defined in Title 18 United States Code, Section 1030(e)(2)(B), thereby causing loss aggregating at least $5,000 in value and causing damage affecting ten or more protected computers during a one-year period beginning on or about February 1, 2019.

COUNT SEVEN

[18 U.S.C. § 2511(a)]

Between or about February 2019 and September 2020, in Los Angeles County, within the Central District of California, and elsewhere, defendants ALEKSANDR STEPANOV, also known as ("aka") "JimBee," aka "Clay Barton," aka "Monster," and DANIL KHALITOV, aka "Flawless," aka "Dancho," intentionally intercepted and endeavored to intercept electronic communications.

COUNT EIGHT

[18 U.S.C. § 2511(d)]

Between or about February 2019 and September 2020, in Los Angeles County, within the Central District of California, and elsewhere, defendants ALEKSANDR STEPANOV, also known as ("aka") "JimBee," aka "Clay Barton," aka "Monster," and DANIL KHALITOV, aka "Flawless," aka "Dancho," intentionally used and endeavored to use the contents of electronic communications, knowing and having reason to know that the information was obtained through the interception of electronic communications in violation of 18 U.S.C. § 2511(1).

FORFEITURE ALLEGATION ONE

[18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c)]

1. Pursuant to Rule 32.2 of the Federal Rules of Criminal Procedure, notice is hereby given that the United States of America will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), in the event of any defendant's conviction of the offenses set forth in any of Counts One through Three of this Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

(a) All right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds traceable to the offenses; and

(b) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraph (a).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c), any defendant so convicted shall forfeit substitute property, up to the value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph or any portion thereof (a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to, or deposited with a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been substantially diminished in value; or (e) has been commingled with other property that cannot be divided without difficulty.

FORFEITURE ALLEGATION TWO

[18 U.S.C. § 982]

1. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal Procedure, notice is hereby given that the United States of America will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Section 982(a)(2), in the event of any defendant's conviction of the offense set forth in Count Four of this Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

(a) All right, title and interest in any and all property, real or personal, constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of the offense; and

(b) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraph (a).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b), any defendant so convicted shall forfeit substitute property, up to the total value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph, or any portion thereof: (a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to or deposited with a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been substantially diminished in value; or (e) has been commingled with other property that cannot be divided without difficulty.

FORFEITURE ALLEGATION THREE

[18 U.S.C. §§ 982 and 1030]

1. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal Procedure, notice is hereby given that the United States will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Sections 982(a)(2) and 1030, and Title 28, United States Code, Section 2461(c), in the event of any defendant's conviction of the offenses set forth in either of Counts Five or Six of this Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

(a) All right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of the offense;

(b) Any property used or intended to be used to commit the offense; and

(c) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraphs (a) and (b).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and 1030(i), the convicted defendant shall forfeit substitute property, up to the total value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph, or any portion thereof: (a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to or deposited with a

third party; (c) has been placed beyond the jurisdiction of the court; (d) has been substantially diminished in value; or (e) has been commingled with other property that cannot be divided without difficulty.

FORFEITURE ALLEGATION FOUR

[18 U.S.C. § 2513 and 28 U.S.C. § 2461(c)]

1. Pursuant to Rule 32.2 of the Federal Rules of Criminal Procedure, notice is hereby given that the United States of America will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Section 2513 and Title 28, United States Code, Section 2461(c), in the event of any defendant's conviction of the offenses set forth in either of Counts Seven or Eight of this Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

(a) All right, title, and interest in any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of 18 U.S.C. §§ 2511 or 2512; and

(b) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraph (a).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c), any defendant so convicted shall forfeit substitute property, up to the value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph or any portion thereof (a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to, or deposited with a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been

//

substantially diminished in value; or (e) has been commingled with other property that cannot be divided without difficulty.

A TRUE BILL

/S/
Foreperson

E. MARTIN ESTRADA
United States Attorney

CHRISTOPHER D. GRIGG
Assistant United States Attorney
Chief, National Security Division

CAMERON L. SCHROEDER
Assistant United States Attorney
Chief, Cyber & Intellectual Property Crimes Section