IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Holding a Criminal Term
Grand Jury Sworn in on May 3, 2018

UNITED STATES OF AMERICA v. MATJAZ SKORJANC, a/k/a "Iserdo," a/k/a "Serdo," FLORENCIO CARRO RUIZ, a/k/a "NeTK," a/k/a Netkairo, MENTOR LENIQI, a/k/a Leniqi Mentor, a/k/a "Iceman," and THOMAS KENNEDY MCCORMICK, a/k/a "Fubar," *Defendants*.	CRIMINAL NO. MAGISTRATE NO. 11-MJ-321 GRAND JURY ORIGINAL VIOLATIONS: 18 U.S.C. § 1962(d) (Conspiracy to Participate in a Racketeering Influenced Corrupt Organization) 18 U.S.C. § 1349 (Conspiracy to Commit Bank Fraud and Wire Fraud) 18 U.S.C. § 1028A (Aggravated Identity Theft) 18 U.S.C. § 2 (Aiding and Abetting) 18 U.S.C. §§ 981(a)(1)(C), 982(a)(2)(A) (Forfeiture)

INDICTMENT

The Grand Jury charges that:

INTRODUCTION

At all times relevant to this Indictment:

1. Defendants MATJAZ SKORJANC, FLORENCIO CARRO RUIZ, MENTOR LENIQI, and THOMAS KENNEDY MCCORMICK, and others known and unknown to the grand jury, were members of a criminal organization engaged in widespread fraud against banks in the District of Columbia and elsewhere and widespread intrusions into computers in the District of

Columbia and elsewhere. The criminal organization centered around an exclusive online forum and marketplace – known as Darkode – for criminals to develop and share hacking tools and schemes. Between at least September 2008, when SKORJANC founded Darkode, and December 5, 2013, when FBI contacted MCCORMICK about his role as an Administrator of Darkode (and searched and seized digital devices from MCCORMICK containing, among other things, financial account access devices and means of identification of numerous victims), this criminal organization defrauded and it's criminal customers, numerous individuals and institutions, including numerous banks, in various schemes, which resulted in a fraud loss of at least $4.5 million. The schemes included selling and using tools – malware – to hack into victim computers and steal personally identifying information ("PII"), bank account and other login credentials, and credit cards. The schemes also included developing and selling tools – malware – for taking over victims' computers and using them to attack victims' web sites; hold victims' websites for ransom; and hide the criminals' identities on the internet.

2. Defendant MATJAZ SKORJANC ("SKORJANC"), also known as "Iserdo," also known as "Serdo," was a citizen and resident of Slovenia.

3. Defendant FLORENCIO CARRO RUIZ ("RUIZ"), also known as "NeTK," also known as "Netkairo," was a citizen and resident of Spain.

4. Defendant MENTOR LENIQI ("LENIQI"), also known as "Leniqi Mentor," also known as "Iceman," was a citizen of Serbia residing in Slovenia.

5. Defendant THOMAS KENNEDY MCCORMICK ("MCCORMICK"), also known as "Fubar," was a citizen and resident of the United States of America.

6. Victim ME was a resident of the District of Columbia.

7. Victim PM was a resident of the District of Columbia.

8. Victim MLB was a resident of the District of Columbia.

9. Victim BC was a resident of the District of Columbia.

10. Victim LC was a resident of the District of Columbia.

11. The "Internet" is a global network connecting millions of computers and computer networks to each other, allowing them to communicate and transfer information. Using, among other things, a system of wires, cables, routers, and circuits, the Internet allows the communication and transfer of information in interstate and foreign commerce.

12. A "bot" is a software program that acts as an agent for a user. It can convert an infected computer to act as a robot for another controller. Bots can also be programmed to function in a malicious capacity, and can operate without any outward sign that would alert the user to their presence. For example, crawler bots are programs used for searching the Internet. As another example, a malicious bot can instruct a computer to send spam, or participate in a cyber-attack against a website without the user's knowledge. A bot can also be used to harvest and transmit the user's passwords and personal information. Bots are a favored tool of cybercriminals because the software on the personal computer and the unauthorized network activity are difficult to detect. After they are in place, bots are very difficult to remove because they are generally designed to hide themselves from virus scanners and other software tools.

13. A "botnet" is a network of computers infected with bots that are used to control or attack computer systems. It typically consists of computers that have been infected with malicious computer software, such as viruses, Trojans, and worms. Botnets are often created by spreading a computer virus or worm that propagates throughout the Internet, gaining unauthorized access to computers on the Internet, and infecting the computer with a particular bot program. The botnet is then controlled by a user, often using a specified channel on Internet Relay Chat. A botnet can

consist of tens of thousands, even millions, of infected computers. The bot code allows infected computers to be remotely controlled by a master computer, commonly referred to as the command and control server. The collection of these computers forms a "bot" network, from which the abbreviation "botnet" is derived. The unsuspecting infected or compromised computers are often referred to as "zombies" or "drones."

14. Botnets are used in furtherance of a variety of criminal conduct, including, for example, (1) the launching of distributed denial of service attacks (DDOS) designed to disrupt and disable targeted computer systems, (2) "phishing," or the use of a clone website that looks like a legitimate website, soliciting the input of personal information such as passwords or bank account numbers, (3) gaining unauthorized access to a computer in order to connect to the Internet, known as a "Socks4/5" server or proxy, or (4) "password harvesting," which involves the unauthorized access to passwords stored on a computer.

15. A distributed denial of service attack or "DDOS attack" is a type of malicious computer activity where an attacker causes a network of compromised computers to "flood" a victim computer with large amounts of data or specified computer commands. A DDOS attack typically renders the victim computer unable to handle legitimate network traffic and often the victim computer will be unable to perform its intended function. The goal of such an attack is to deny legitimate users the services of the computer. Depending on the type and intensity of the DDOS attack, the victim computer and its network may become completely disabled and require significant repair.

16. "Password harvesting" is the practice of gathering and collecting online login credentials and credit card numbers. Criminals generally do so in order to sell the credentials, often in bulk. Internet forums are used by criminals around the world to sell and trade credentials

based on various characteristics. One subject may specialize in fraud associated with credit card information, while another may primarily use Internet banking credentials. Criminals trade illicitly-gathered information based on the type of credential, the bank or establishment associated with the credential, the country associated with the credential, or how recently the credentials were stolen. Credentials are priced in different tiers based on such characteristics and sold or traded for profit in criminal Internet forums.

17. A "domain" is a set of subjects and objects on the Internet that share common security policies, procedures, and rules, and are managed by the same management system. A "domain name" identifies where on the World Wide Web the domain is located. A "domain name server" or "DNS" translates or maps domain names to Internet Protocol ("IP") addresses and vice versa. Domain name servers maintain central lists of domain names/IP addresses, translate or map the domain names in an Internet request, and then send the request to other servers on the Internet until the specified address is found.

18. An "Internet protocol address" or "IP address" is a unique numeric address used by computers on the Internet. An IP address is designated by a series of four numbers, each in the range 0-255, separated by periods (e.g., 2.56.97.78). Every computer connected to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet Service Providers control a range of IP addresses, which they assign to their subscribers. No two computers directly connected to the Internet can have the same IP address at the same time. Thus, as a general matter, at any given moment an IP address is unique to the computer to which it has been assigned.

19. A "server" or "box" is a centralized computer that provides services for other

computers connected to it via a network. The other computers attached to a server are sometimes called "clients." In a large company, it is common for individual employees to have client computers on their desktops. When the employees access their email, or access files stored on the network itself, those files are pulled electronically from the server where they are stored, and are sent to the client's computer via the network. In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a World Wide Web site is known simply as a "web server." Similarly, a server that only stores and processes email is known as a "mail server."

20. "Spam" generally is an email message that is sent in bulk to recipients without prior request or approval. The origin of the spam is usually masked or falsified to prevent any identification of the sender.

21. "Malware" is an abbreviated term for "malicious software." Malware refers to software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, worms, Trojan horses, and spyware. Malware can gather data from a user's system without the user knowing it.

22. "Ransomware" is a type of malware that prevents users from accessing their computer system or files and demands ransom payment in order to regain access.

23. The "Dark Web" refers to a collection of websites and computers that are deliberately hidden from general public access. Unlike the ordinary part of the internet, the Dark Web assures anonymity for those who access it. Although the Dark Web may be used for legitimate purposes, it also attracts those who would use the computer for criminal purposes, primarily because the layers of encryption assure anonymity of its users.

24. The Onion Router ("TOR") is a tool used to access and place computers and

marketplaces and forums on the Dark Web. The basis for acronym TOR ("the onion router") refers to the layers of encryption used to assure anonymity.

COUNT ONE
(Racketeer Influenced Corrupt Organization Conspiracy)

25. Paragraphs 1 – 24 are hereby incorporated and re-alleged herein.

The Racketeering Conspiracy

THE ENTERPRISE

26. At various times relevant to this Indictment, the defendants MATJAZ SKORJANC, FLORENCIO CARRO RUIZ, MENTOR LENIQI, and THOMAS KENNEDY MCCORMICK, together and with others known and unknown to the grand jury, were members and associates of the Darkode forum, an invitation-only online forum which was a criminal organization whose members and associates engaged in, among other things, bank fraud, wire fraud, computer fraud, access device fraud, identity theft, and extortion.

27. The Darkode forum, including its leaders, members, and associates, constituted an Enterprise, as that term is defined in Title 18, United States Code, Section 1961(4), that is, a group of individuals associated in fact. The Enterprise constituted an ongoing organization whose members functioned as a continuing unit for a common purpose of achieving the objectives of the Enterprise. The Enterprise was engaged in, and its activities affected, interstate and foreign commerce.

28. The Enterprise, which operated in the District of Columbia and the countries of Spain, Slovenia, and elsewhere, operated through groups of individuals responsible for the various computer intrusions, fraudulent schemes, and criminal activities. While the overall structure and model of the Enterprise remained constant, the members' responsibilities within the overall structure of the Enterprise were in a state of flux to adjust for the specific needs of the specific

criminal activity of the Enterprise. In particular, the defendants and others organized a forum over the internet, known as "Darkode," to facilitate the exchange of ideas, knowledge, and advice, in computer related criminal activity, and to provide a tightly controlled marketplace for buyers and sellers engaged in computer related criminal activity.

29. Darkode's home page was located on the internet at http://darkode.com. It was comprised primarily of users who were interested in the use, sale, and deployment of malware for the purpose of generating revenue. The forum was run by an Administrator, and a succession of Administrators, from at least 2008 until approximately the beginning of December 2013. SKORJANC was the first Administrator and MCCORMICK was one of the last.

30. Members of Darkode were carefully vetted through an elaborate process and access was restricted to only vetted members, that is, by invitation only.

THE RACKETEERING VIOLATION

31. Between the end of September, 2008, through December 5, 2013, within the District of Columbia, and in the countries of Spain, Slovenia, and elsewhere, at various times relevant to this indictment, the defendants MATJAZ SKORJANC, FLORENCIO CARRO RUIZ, MENTOR LENIQI, and THOMAS KENNEDY MCCORMICK, together and with others known and unknown to the grand jury, being persons employed by and associated with the Darkode forum, described above, an Enterprise which engaged in, and the activities of which affected, interstate and foreign commerce, knowingly and intentionally conspired to violate 18 U.S.C. § 1962(c), that is, to conduct and participate, directly and indirectly, in the conduct of the affairs of said Enterprise through a pattern of racketeering activity, as defined in 18 U.S.C. §§ 1961(1) and (5) consisting of multiple acts indictable under the following provisions of federal law:

a. 18 U.S.C. § 1951 (relating to interference with commerce, robbery, or

extortion);

b. 18 U.S.C. § 1343 (relating to wire fraud);

c. 18 U.S.C. § 1344 (relating to financial institution fraud);

d. 18 U.S.C. § 1029 (relating to fraud and related activity in connection with access devices);

e. 18 U.S.C. § 1028 (relating to fraud and related activity in connection with identification documents);

f. 18 U.S.C. § 1030(a)(1) (relating to the protection of computers); and

g. 18 U.S.C. § 1030(a)(5)(A) (resulting in damage as defined in §1030(c)(4)(A)(i)(II) through (VI)).

32. It was a part of the conspiracy that each defendant agreed that a conspirator would commit at least two acts of racketeering activity in the conduct of the affairs of the Enterprise.

PURPOSES OF THE ENTERPRISE

33. The purposes of the Enterprise included but were not limited to the following:

a. to generate money for its members and associates. This purpose was implemented by members and associates of the Enterprise through the commission of various criminal acts including: bank fraud, wire fraud, computer fraud, access device fraud, identity theft, extortion and various forms of computer intrusions;

b. to preserve and protect the ability of the Enterprise to enrich its members and associates through the corrupt use of false and fictitious identities and entities to hinder detection by law enforcement; and

c. to promote and enhance the criminal activities of the Enterprise and its members and associates;

d. to protect the Enterprise and its members from detection, apprehension and prosecution by law enforcement;

e. to preserve and enhance the reputation, operations and profits of the Enterprise through discipline, expulsion, and other acts of retribution against non-conforming members.

34. The Enterprise was bound together by, among other things, the members' and associates' common interest, knowledge, and usage of the Internet, computer, and their vulnerabilities to fraudulently obtain money from victims pursuant to various fraudulent schemes, including but not limited to, schemes to steal bank information using malicious programs, to extort website and computer owners through DDOS attacks and ransomware attacks, and to sell access to compromised computers (botnets) to other forum members seeking to install their own malicious programs.

MANNER AND MEANS OF THE ENTERPRISE

35. The manner and means by which the defendants and their associates conducted and participated in the conduct of the affairs of the Enterprise included, but are not limited to the following:

a. On or about the beginning of September 2008, the exact date being unknown to the grand jury, the Darkode forum was created and registered on the internet with a website (home page) at http://darkode.com. At some point after 2013, the forum moved to a section of the web known as the Dark Web or TOR (the onion router).

b. Darkode promoted itself as the "Best Malware Marketplace on the Net." The Darkode forum sought to generate money for its members and associates. Its members consisted of those computer users who were interested in the use, development, creation, sale, and

deployment of malware for the purpose of generating revenue. Over the forum, members worked collaboratively to use each other's skills and products to create, modify, and improve software designed to infect computers and electronic devices. Members could also create their own malware independently and offer it for sale on the Darkode forum. They collaborated over the forum website to create programs to gain access to and control over computers and devices including those computers hosting websites. They would post finished malware products for sale on other websites (like those accessible to the public) and would post finished "hacker" products for sale to other members of the Darkode forum.

c. Members of Darkode were carefully vetted through a two-step process. First, a prospective member had to have been invited to the forum by an existing member. Next, the prospective member had to post an introduction on the Darkode forum. The introduction typically included the types of criminal activity in which the new user sought to engage. This process of vetting prospective members assured that only those with the requisite skills or products would achieve membership. The selective inclusion also assured that only those with a shared criminal interest in computer hacking activities would be able to participate in the Darkode forum. If existing members vouched for the new member, the new member was allowed full access to the Darkode forum. The membership of the Darkode proved to be international. Still, access to and membership in the Darkode forum was intentionally restricted; it was by invitation only. Furthermore, member conduct was regulated. An Administrator of the Darkode forum could revoke a member's access and thereby regulate or punish a member's behavior that was deemed unacceptable.

d. In order to facilitate the operation of Darkode, certain members rose in prominence and assumed management duties of the Darkode forum. SKORJANC emerged as

the first Administrator of the Darkode. The Administrator served as a manager and controller of activities on the forum. The Administrator had authority to eject a member by revoking his/her access. His leadership extended from September 2008 to at least until March 2010. SKORJANC was recognized on the Darkode using the moniker "Iserdo," There followed a succession of Administrators. Members participated and communicated on the Darkode usually using monikers. MCCORMICK using the moniker "Fubar," emerged as one of the last Administrators of the Darkode. He was accepted as a member as early as 2009. The Administrator of the Darkode forum acted to assure the overall success of the forum, moderated and managing forum conversation threads for selling and providing the latest malware, managed efforts of the forum to create or render malware undetectable to antivirus software currently on the market or currently in use, facilitated access to botnets, facilitated the creation of infrastructure to host a botnet known as bulletproof hosting and bulletproof domains, provided other members with access to databases of stolen PII like names, social security numbers, dates of birth, email lists for spam, and to provide access to compromised servers. At times, the Administrator would broker sales of malware on behalf of a creator member of the forum. Also, the Administrator would resolve or attempt to resolve complaints by members of the forum when there were disputes about sharing proceeds from criminal profit-making activities.

e. Members strove to achieve anonymity in order to evade detection by law enforcement. In order to preserve anonymity, even among themselves, members were careful to interact online using their email monikers, e.g., iserdo@gmail.com.

f. Members usually avoided monetary transactions that might reveal the identity of those involved. Proceeds of the sale of botnet and malware activities often

involved internet money processors. Beginning with SKORJANC and continuing through with MCCORMICK they and others in the forum preferred to use internet money processors such as Liberty Reserve and Webmoney. Occasionally, forum members used money remitters like Western Union to purchase money orders or to conduct wire transfers. Many forum members were careful to avoid using ordinary financial institutions like banks to pay for malware because such institutions did not assure anonymity, that is, they usually required disclosure of real world identities. For example, MCCORMICK was careful not to accept wire transfers for payment as such transactions often required the payor to identify the recipient of the transfer and the remitter would require the recipient to produce documentation of their identity (like a driver's license) when picking up the funds from such a transfer. MCCORMICK was also careful not to cash out proceeds from his online criminal computer activity and avoided the exchange of virtual currencies to a debit/credit card, as such transactions often revealed the real world identity of the recipient.

g. In addition, members regularly used encrypted internet chat programs to protect their communications from interception and/or to evade detection by law enforcement. Jabber and Microsoft Instant ("MSN") Messenger, were among the types of software that permitted users to "chat" online in real time, in contrast with email. P2P (Peer-to-Peer) computing or networking software was often used by members to facilitate the transfer of data between computers.

h. To achieve the goals of the conspiracy and generate revenue, members were permitted to list malware on the Darkode website even if it had not been created in cooperation with another member.

i. Members advertised their malware creations, including botnets, on the

Darkode forum. For example, SKORJANC created a bot software known as Butterfly Bot ("BFBOT"). By October 2008, he had listed it for sale on Darkode at a price of 350 Euros for the basic version, and he would accept payment at that time by Western Union or other "money brokers." The posting on Darkode listed the overall description and purpose of the BFBOT as follows:

> Bot designed to stealthy run on winnt based systems (win2k to winvista) and to stealthy and efficiently spread via 3 above mentioned methods, which were specially designed and improved compared to already known public methods. The bots purpose is not attacking, phishing, stealing person info or servin as socks server. All these features can be added for additional price or uploaded and executed on bot (as it supports download command).

SKORJANC advertised the bot as the "newest product that is modular in nature," that is, he allowed customers to choose specific capabilities of the botnet software. He advertised that the software also had the capability to steal sensitive information including usernames and passwords for banks and other financial institutions from users of Firefox and Internet Explorer web browsers and included DDOS features. SKORJANC explained that the BFBOT was capable of infecting any version of MSN Messenger, and was capable of altering the text entered into MSN Messenger. SKORJANC advertised that the BFBOT was undetectable on novirusthanks.org, a website that permitted the public to scan a given software file with a number of antivirus products.

j. Another example of advertisements for malware on Darkode was that, on or before December 2009, RUIZ advertised on the Darkode website that he was selling access to his botnet. This botnet was known as the Mariposa botnet, which was a customized version of the Butterfly Bot (BFBOT) created by SKORJANC. SKORJANC and RUIZ collaborated to refine the Mariposa botnet.

k. RUIZ also used the Mariposa botnet himself to execute a DDOS attack on website www.telegrow.com for the purpose of extortion. In exchange for stopping the attack, RUIZ demanded payment of 1,000 Euros.

l. Members of Darkode shared access to compromised computers, which enabled others to use an existing botnet to upload and install malicious software, called "installs," and were negotiated on a price per computer. For example, RUIZ profited by selling access to compromised computers that were part of his Mariposa botnet. The Mariposa botnet resulted in 2.6 million IP addresses compromised simultaneously and over ten million computers with unique IP addresses eventually compromised by this botnet. Of those 2.6 million IP addresses identified as compromised, 400,000 were identified as belonging to IPs in the United States. Of those 400,000 compromised IP addresses, 5,700 were registered to entities in Washington, D.C., and six of those entities were registered to United States Government entities in Washington, D.C.

m. To achieve the goals of the conspiracy and generate revenue, members not only marketed malware on the Darkode forum, they communicated with each other to assure that the malware would accomplish the criminal purposes intended. For example, in April 2010, LENIQI negotiated, for $60, the sale of thirteen compromised servers for which he had illegally obtained full administrative access. The buyer was a person communicating with LENIQI through a server located in Washington, D.C. LENIQI explained that the compromised servers were located in several different datacenters in the United States, Europe, Russia, and China. The sale was completed over the internet payment processor PayPal. In support of the sale, LENIQI explained that he had purchased the BFBOT from SKORJANC and used that malicious software to create his own botnet, which he was now

using to sell access to others on the Darkode forum.

n. LENIQI had purchased a version of the BFBOT, called the Butterfly Flooder Bot from SKORJANC because he was interested in using the bot to conduct DDOS attacks. Before acquiring the Butterfly Flooder Bot, on January 9, 2010, LENIQI discussed with RUIZ the capabilities of the Butterfly Flooder Bot. RUIZ assured LENIQI that it possessed capabilities of launching a strong DDOS attack. On January 11, 2010, LENIQI contacted SKORJANC who agreed to sell the Butterfly Flooder Bot software for 500 Euro, which funds were sent to a bank account located in Maribor, Slovenia. In such conversations, the members of the Darkode forum could and did openly discuss their criminal intentions. They could obtain assurance from other Darkode forum members of the quality of malware offered for sale on the Darkode forum, and conduct transactions with assurance that the malware would accomplish the criminal tasks for which the buyer intended. In such manner, members of the Darkode forum could exchange ideas, knowledge, and advice, with assurance that the forum would provide a tightly controlled marketplace for buyers and sellers of computer malware.

o. Darkode forum members also worked collaboratively to assist each other in the sale of malware. For example, between December 14, 2009 and January 15, 2010, another person, acting in undercover capacity for the Federal Bureau of Investigation ("FBI"), posed as a member of the Darkode forum and purchased the Zeus malware from MCCORMICK. The two identified each other over the Darkode forum website and continued to transact the sale of the Zeus malware by continuing conversations over an internet chat program. Over the internet chat program, MCCORMICK stated that he was offering to sell "installs" and he would also assist with the sale of Zeus. Zeus, also known as Zeus Trojan or

Zeus Bot, was malware used to harvest banking credentials from victims for the purpose of electronically stealing funds from those victims. MCCORMICK agreed to facilitate the sale of Zeus malware on behalf of its author and therefore directed the purchaser to send $7,200 to the Webmoney account belonging to the author. When the transaction was verified, MCCORMICK supplied the purchaser with a link to download the malicious software. The Zeus malware was so effective that, by August 2009, it had been used to infect 60,000 computers, which were used to generate stolen data from users of those computers and others approximately 200 million times, giving the Zeus creator and his customers' access to unique PII and bank account credentials and information.

p. In another instance illustrative of collaborative effort, in which forum members would work together to engage in criminal profit making activities, MCCORMICK associated with another forum member identified as "Solotech," to engage in bank fraud. The two created software known as a "cookie cleaner" malware program which, when inserted into a computer, would force the victim who was using the infected computer to log back on to a bank account by clearing the bank connection session before completion. Once the victim logged back in to establish the banking connection, the malware would harvest (capture) PII, including the victim's username, password, PIN numbers, and answers to security questions. Using the malware, the two were able to obtain large quantities of PII, which was later used to commit bank fraud.

q. Members also collaborated in documenting how to use the malware that they designed. The manual for BFBOT v1.5 listed SKORJANC as the developer and primary contact for the Butterfly Bot 1. The Spanish language version of the same manual listed RUIZ as the contact for BFBOT for Spanish speakers. Both manuals included instructions on how to use

the password POST data grabber. A POST data grabber is a tool for harvesting victims' login credentials.

r. MCCORMICK, alone and in collaboration with other forum members, also participated in pay-per-install activity, that is he and others installed ransomware by means of a pay-per-install affiliate program, and sold "installs" to others.

s. Members of the Darkode forum generated so much stolen PII and banking credentials that they frequently used external digital storage devices to retain all the data. MCCORMICK used various external storage devices, like thumb drives and microSD cards (digital storage devices like the memory card used in digital cameras), to retain the stolen credentials. These devices often had Structure Query Language (SQL) databases commonly used for managing large amounts of data, which they used to store thousands of usernames and passwords. Such storage allowed easy access, which in turn, allowed them to use this data for hundreds or thousands of fraudulent transactions. On December 5, 2013, MCCORMICK possessed a USB thumb drive that contained stolen credit card information, bank login data, and PII such as name, address, phone number, dates of birth, and account names and numbers. MCCORMICK's drive contained over 30,000 credit/debit card numbers belonging to over 1,600 financial institutions. Analysis revealed 21,639 verified compromised accounts including 13,070 Visa; 5,292 MasterCard; 2,132 American Express; and 1,145 Discover card accounts. The credit/debit card numbers belonged to victim bank institutions including Bank of America (2,960 accounts), JP Morgan Chase (2,805 accounts), and Wells Fargo/Wachovia (1,519 accounts). Investigation of the compromised American Express accounts on MCCORMICK's seized thumb drive revealed that American Express reported $312,461 in fraud associated with the 2,132 accounts. JP Morgan Chase reported that there was $366,532 in fraud associated with the

2,805 stolen accounts on the thumb drive. Thus, the fraud amount evidence found in the thumb drive was at least $678,993.

t. On December 5, 2013, MCCORMICK also possessed a microSD card. It contained files on ngrBot. The ngrBot was malware created by MCCORMICK in association with two others from the Darkode forum and was advertised for sale on the Darkode website. MCCORMICK acted as the sales manager for ngrBot. The ngrBot functioned as a computer hacker tool with a multitude of features to facilitate fraud through the theft of PII and banking credentials. The ngrBot allowed for the stealthy execution of a file downloaded to a victim computer. The ngrBot malware was designed to avoid detection by antivirus software currently available on the market. The ngrBot features included: a proactive defense to remove competing malware; a DNS modifier which blocked domains on infected computers and prevented antivirus updates; functionality to initiate a distributed denial of service attack against a web site or webserver; Internet Explorer and Firefox browser key loggers (which are used to capture usernames and passwords); functionality to spread malware via USB devices such as removable media and external hard drives; and, a functionality to spread malware via MSN Messenger—that is, it was designed to spread malware through MSN Messenger, an instant messaging software program. All such features of ngrBot were designed to infiltrate a victim computer, spread malware, and to steal PII and banking credentials, which in turn can be used to commit fraud.

OVERT ACTS

36. In furtherance of the conspiracy, and to achieve the object and purposes thereof, in the District of Columbia, and elsewhere, including Spain and Slovenia, the defendants, and others known and unknown to the grand jury, performed or caused to be performed the

following overt acts, among others:

37. On November 9, 2008, SKORJANC in an email conversation with a new member of the Darkode forum identified himself as "the Management."

38. On November 9, 2008, SKORJANC in an email conversation with a new member of the Darkode forum provided a new member with instructions on how to access the Darkode.

39. On August 3, 2009, a Darkode member identified as M4, explained the need to avoid detection by law enforcement and stated to another Darkode member the need to use instant messaging encryption:

> Many people discuss not so legal stuff over Instant Messengers which can be seen in plain text. The most don't give a fuck and tease the faith. What about you? My opion that it should be a must, using SIMP f.e., to encrypt your IM traffic and keep your conversation in privacy on such kind of forums. Just in case…to do not tease the faith. P.S. would be good if all the people from this forum I have on my MSN list got SIMP or any other relative tool.

40. From on or before September, 2008, and continuing thereafter until on or about May 26, 2010, DP (a Darkode forum member whose identity is known to the grand jury but not indicted herein, a/k/a Nocen, a/k/a Loki, a/k/a Juggernaut, a/k/a MlrrOr), conspired and agreed together with SKORJANC, and others both known and unknown to the grand jury, to access a computer without authorization and thereby obtain information from a protected computer.

41. On or about June 15, 2009, SKORJANC advertised on Darkode that, "My coding skills are for sale. I have made numerous malware relate projects. … I have a lot of malware coding experiences and so I can also advise you what to do/use. I ACCEPT ONLY PROJECTS WORTH 1000 EUR OR MORE!" SKORJANC then said that he had made a POST

data grabber for Internet explorer versions 6 through 8. Another Darkode user responded that "you wanna have a costum project done than iserdo is your man my hidden link sender coded by iserdo is afther all the time i have it onley detacted by 2 av [anti-virus]."

42. On or about January 5, 2010, DP agreed to sell malware that he designed to monitor and harvest network traffic for email addresses and passwords to an individual known as Dethan.

43. Beginning on or about January 5, 2010, DP conducted several internet chats with a person known as Dethan, in which he offered advice on how to maximize the effectiveness of the software (by running it on the same machine as a spam bot, for example, to capture all of the spammer's email addresses, or to run it on a mail server).

44. On January 16, 2010, on the Darkode forum, a new member, identifying himself as Gribodemon, "the author of new banking malware," SpyEye (and whose identity is known to the grand jury but not indicted herein as Aleksandr Andreevich Panin, who pled guilty to charges related to the development of that malware on January 28, 2014), started a thread on Darkode called "SpyEye author is here." SpyEye was designed to automate the theft of confidential personal and financial information, such as online banking credentials and the victims' stolen personal and financial data was then surreptitiously transmitted to the C2 servers, where it was used to, among other things, steal money from the victims' financial accounts. RUIZ wrote "wellcome we talk!! :D" to Gribodemon. MCCORMICK also welcomed the new member, writing, "welcome man, i was talking to you on icq before (mine is 979703)."

45. On or about March 13, 2010, LENIQI responded to a Darkode user (who had posted an ad for a keylogger that captured banking credentials), stating that the keylogger is

"very recommended."

46. On or about May 26, 2010, DP possessed a computer that contained rootkits, botnets, and spamming programs and fully functional websites that were templates for spam affiliate programs. "Rootkits" are malware that allow criminals to seize full administrative control of a computer.

47. On or about May 26, 2010, DP possessed fifteen or more stolen access devices, that is, a computer that contained files with 74,190 credit card numbers and 297 bank account numbers which were stolen.

The Butterfly Bot

48. Between on or about September 29, 2008 and continuing up to or about July 2010, SKORJANC listed the Butterfly Bot (BFBOT) malware for sale on the Darkode forum.

49. From on or about September 29, 2008, and continuing up to in or about July 20 2010, the defendants, SKORJANC, RUIZ, LENIQI, and others known and unknown to the grand jury, caused the transmission of a program, known as BFBOT, to gain unauthorized access to, and control over, victims' computers.

50. On or about October 28, 2008, SKORJANC posted the BFBOT malware for sale along with the various modules (allowing for customers to pick and choose among its various malware specialties like DDOS, harvesting banking credentials, and self-propagation) on a website www.unk.bz for sale for 350 Euros which was described as follows:

> Bot designed to stealthy run on winnt based systems (win2k to winvista) and to stealthy and efficiently spread via 3 above mentioned methods, which were specially designed and improved compared to already known public methods. The bots purpose is not attacking, phishing, stealing person info or servin as socks server. All these features can be added for additional price or uploaded and executed on bot (as it supports download command).

51. On or about November 3, 2009, SKORJANC told Darkode users that he had already created a POST data grabber module for the Butterfly Bot.

52. On November 11, 2009, in a Darkode thread, MCCORMICK wrote that a custom add-on for the Butterfly Bot will cost "400 EUR or 600 USD (payment: Western Union) *only avaliable with purchase of BFBOT software."

53. On or about December 29, 2009, SKORJANC advertised a POST data grabber for the Butterfly Bot for 200 Euros.

54. On or about December 30, 2009, SKORJANC announced that the new POST data grabber module was "tested and working."

55. On or about June 27, 2010, a Darkode member identified as M7, posted a message on the Darkode forum on the thread BFBOT Pro 1.51, advertising to other members the sale of a botnet consisting of 900 victim computers:

> I am putting this up again because last time the buyer didn't went through, there fore I still have the bot. It comes with the 3 domains, and right now it has 900 bots online. Price 20$ today (discussable). Payment via LR/WMZ [Liberty Reserve/Web Money]. Forgot to mention it comes with a hacked offshore server (been using it for months and months. Unfortunately I am in a rush to make a quick buck, and since I haven't been using BFBot for quite some time, I will let it go for 90$ right now.

The Butterfly Flooder Bot

56. On or about November 18, 2009, SKORJANC told LENIQI that SKORJANC was the only person developing the Butterfly Flooder Bot.

57. On or about November 20, 2009, SKORJANC offered to sell LENIQI the Butterfly Flooder Bot for a discounted price of 500 Euros because LENIQI had previously bought the Butterfly Bot.

58. On or about January 11, 2010, LENIQI agreed to purchase the Butterfly Flooder Bot, which was a new version of the BFBOT, for 500 Euros from SKORJANC.

59. On or about January 11, 2010, LENIQI asked SKORJANC if the Butterfly Flooder Bot had a tool for grabbing login credentials. SKORJANC wrote that it had a tool for stealing login credentials from banks and PayPal, the POST data grabber. SKORJANC offered to sell LENIQI the POST data grabber for 200 Euros.

60. On or about January 12, 2010, LENIQI told SKORJANC that he had bank wire transferred 250 Euro to SKORJANC.

61. On or about February 16, 2010, LENIQI told SKORJANC that he had bank wire transferred the remaining funds to SKORJANC.

62. On or about April 15, 2010, LENIQI advertised on the Darkode website the sale of servers that were compromised.

63. On or about April 15, 2010, LENIQI negotiated the sale, for $60, of access to thirteen compromised servers with an undercover FBI agent posing as a customer. On or about April 15, 2010, after the sale of access to the thirteen compromised servers, LENIQI told the undercover FBI agent that LENIQI had purchased the BFBOT from SKORJANC and used it to create his own botnet.

64. On or about June 2, 2010, LENIQI purchased the Butterfly Flooder Bot POST data grabber, used to steal banking and other login credentials, from SKORJANC.

65. On December 5, 2013, MCCORMICK possessed a microSD card that contained a record of a payment from MCCORMICK to SKORJANC for a copy of the Butterfly Flooder bot for $520.

The Mariposa Botnet

66. Between on or about October 2008 and May 2009, SKORJANC and RUIZ collaborated to customize a version of the BFBOT malware into the Mariposa botnet malware. SKORJANC programmed a POST data grabber and other customizations for RUIZ.

67. Between on or about October 2008, and May 2009, SKORJANC and RUIZ, deployed the Mariposa botnet malware so that by May 2009, it had infected at least 2.6 million computers worldwide – including approximately 400,000 IP addresses in the United States, 5,700 IP addresses were in the District of Columbia, and six IP addresses registered to the United States Government.

68. Between on or about October 2008, and the end of January 2010, RUIZ listed the Mariposa Botnet and its various components for sale on the Darkode forum.

69. On April 29, 2009, RUIZ sent a payment of 400 Euros to Maribor, Slovenia to pay SKORJANC for the configuration of BFBOT used to enhance the performance of the Mariposa botnet.

70. On or about December 17, 2009, RUIZ advertised the sale of installs on the Darkode forum.

71. On or about December 17, 2009, RUIZ responded to an individual with the moniker _0x90u asking if anyone on the forum was willing to sell installs for his malware posting "33k mix if u want pm me" meaning RUIZ had a botnet consisting of 33,000 previously compromised computers located all around the world and if the potential buyer was interested in purchasing access to install his software, he could reach RUIZ by private message via the Darkode forum.

72. On or about January 8, 2010, RUIZ sold access to his botnet for the purpose of installing malware on the compromised computers controlled by RUIZ.

73. Between on or about January 8 and 9, 2010, RUIZ accepted payment of $240 from an agent of the FBI posing as a computer hacker customer so RUIZ would install an executable program (which only reported back to the FBI the IP address of the victim computer) on over 13,000 previously compromised computers worldwide.

74. In or about February 2010, RUIZ possessed a USB drive containing hundreds of thousands of victims' banking and other credentials harvested using the Butterfly Bot. The victims were from all over the world, including the United States. The USB drive also contained a copy of the Zeus malware, which is designed to harvest banking credentials.

75. In or about February 2010, SKORJANC stated to a confidential human source of the FBI posing as a customer (who had asked SKORJANC about the Mariposa botnet):

> I did software for mariposa, its bfbot, but it has connect hook, post data grabber and some google thingie with modified poly engine, thats it.

76. On or before February 2010, RUIZ used the Mariposa botnet to execute a DDOS attack against the website www.telegrow.com and demanded payment to cease the attack.

ngrBot

77. From March 21, 2009 through at least June 11, 2011, MCCORMICK created malware with the assistance of other members of the Darkode forum. MCCORMICK acted as a sales manager for malware, which was called ngrBot, and which functioned as a tool to surreptitiously invade other computers to facilitate DDOS attacks and the theft of PII and banking credentials.

78. Between February 13, 2011 through July 11, 2011, MCCORMICK advertised for sale on the Darkode Forum malware known as ngrBot.

79. On or about December 5, 2013, MCCORMICK possessed a microSD card which recorded certain activity conducted and data transacted on the Darkode forum, including files of 37 unique ngrBot customers.

Zeus

80. From on or about December 14, 2009 through at least December 22, 2009, MCCORMICK advertised via MSN Messenger account root@botnet.biz as follows: "Fubar-Selling latest Zeus."

81. On or about, December 14, 2009 through January 15, 2010, MCCORMICK negotiated the terms of the sale of malware known as Zeus, which was malware, designed to harvest banking credentials from victims for the purpose of electronically stealing funds.

82. On or about January 15, 2010, MCCORMICK acting as an agent/broker for the creator of the Zeus malware, sold it for $7,200 to a person who was acting in an undercover capacity as a customer, but who was in fact, an FBI agent.

McCormick

83. Between or about August 25-27, 2012, MCCORMICK and a Darkode forum member known by the moniker "Snipa," who is known to the Grand Jury but not indicted herein, intruded into a website called ziddu.com and discovered vulnerabilities which allowed them to steal 4.8 million user email addresses and passwords and the two posted their discovery for sale on the Darkode forum.

84. On or about September 13, 2013, MCCORMICK logged on the Darkode forum as Administrator.

85. On December 5, 2013, MCCORMICK possessed fifteen or more unauthorized access devices with the intent to defraud, that is, a USB thumb drive that contained over

30,000 stolen credit/debit card numbers belonging to over 1,600 financial institutions involving 21,639 compromised accounts including 13,070 Visa, 5,292 MasterCard, 2,132 American Express, and 1,145 Discover card accounts with an aggregate fraud loss of at least $678,993.

86. On or before December 5, 2013, MCCORMICK possessed at least 60 credit card numbers, and their respective personal identification information including names, addresses, and phone numbers of residents of the District of Columbia.

(All in violation of Title 18, United States Code, Section 1962(d))

COUNT TWO
(Conspiracy to Commit Bank Fraud and Wire Fraud)

87. Paragraphs 1-24, 26, 29-30, and 36-86 are hereby incorporated and re-alleged herein.

88. From in or about September 2008, and continuing up to in or about December 5, 2013, in the District of Columbia, and elsewhere, including Spain and Slovenia, the defendants, MATJAZ SKORJANC, FLORENCIO CARRO RUIZ, MENTOR LENIQI, and THOMAS KENNEDY MCCORMICK others known and unknown to the grand jury did:

a. knowingly and willfully conspire, combine, confederate, and agree among each other and with other persons to devise a scheme and artifice to defraud and to obtain money and property from individuals and corporations, including financial institutions, by means of false and fraudulent pretenses, representations and promises, using wire communications in interstate and foreign commerce, in violation of Title 18, United States Code, Sections 1343; and

b. knowingly and willfully conspire, combine, confederate and agree among each other and with other persons to execute a scheme and artifice to defraud a financial institution or to obtain any of the moneys funds, credit assets, securities, or other property owned by, or under

the custody or control of, a financial institution, by means of false and fraudulent pretenses, representations and promises, in violation of Title 18, United States Code, Sections 1344.

89. It was part of the conspiracy for the defendants, MATJAZ SKORJANC, FLORENCIO CARRO RUIZ, MENTOR LENIQI, and THOMAS KENNEDY MCCORMICK, and others, to unlawfully enrich themselves by taking over, or aiding and abetting other people to take over, victims' bank accounts.

90. The object of the conspiracy was to be accomplished by the manner and means as described in the lettered sub-paragraphs of Paragraph 35, which are re-alleged and incorporated as if set forth herein.

91. It was part of the conspiracy that the defendants, MATJAZ SKORJANC, FLORENCIO CARRO RUIZ, MENTOR LENIQI, and THOMAS KENNEDY MCCORMICK, and others, would develop, buy, sell, and use malware designed to harvest victims' online banking credentials, which malware would then be used for such purposes.

92. In furtherance of the conspiracy and to carry out its objectives, the defendants and their co-conspirators undertook the acts described in Paragraphs 36–86, which are re-alleged and incorporated as if set forth herein.

(**Conspiracy to Commit Bank Fraud and Wire Fraud**,
in violation of Title 18, United States Code, Section 1349)

COUNTS THREE – SEVEN
(Aggravated Identity Theft)

93. Paragraphs 1-24, 26, 29-30, and 36, 88-91 are hereby incorporated and re-alleged herein.

94. On or about December 5, 2013, within the District of Columbia, the State of Massachusetts and elsewhere, and in the countries of Spain, Slovenia, and elsewhere, THOMAS KENNEDY MCCORMICK, during and relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), that is, Conspiracy to Commit Bank Fraud and Wire Fraud, in violation of Title 18, U.S.C. § 1349, Wire Fraud, in violation of 18 U.S.C. § 1343, Bank Fraud, in violation of 18 U.S.C. § 1344, and Access Device Fraud, in violation of 18 U.S.C. § 1029(a)(3) and (a)(5), did knowingly possess and use without lawful authority, a means of identification of another person, each of whom was a resident of Washington, D.C., that is,

Count	Credit Card Number	Victim
THREE	xxxxxxxxxx89496	ME
FOUR	xxxxxxxxxx78458	PM
FIVE	xxxxxxxxxx15723	MLB
SIX	xxxxxxxxxx56041	BC
SEVEN	xxxxxxxxxx77909	LC

(**Aggravated Identity Theft**, in violation of title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A (c)(4), and (5), Section 2)

FORFEITURE ALLEGATION

Upon conviction of the felony offense charged in Count One of the Indictment, the defendants MATJAZ SKORJANC, FLORENCIO CARRO RUIZ, MENTOR LENIQI, and THOMAS KENNEDY MCCORMICK shall forfeit to the United States (1) any interest acquired or maintained in violation of Title 18, United States Code, Section 1962; (2) any interest in; security of; claim against; or property or contractual right of any kind affording a source of influence over; any enterprise established, operated, controlled, conducted, or participated in the conduct of, in violation of Title 18, United States Code, Section 1962, and (3) any property constituting, or derived from, any proceeds obtained, directly or indirectly, from racketeering activity in violation of title 18, United States Code Section 1962;

Upon conviction of the felony offense alleged in Count Two, the defendants MATJAZ SKORJANC, FLORENCIO CARRO RUIZ, MENTOR LENIQI, and THOMAS KENNEDY MCCORMICK shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to this offense, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 461(c). The United States will also seek a forfeiture money judgment against the defendant equal to the value of any property, real or personal, which constitutes or is derived from proceeds traceable to these offenses.

Upon conviction of any of the felony offenses alleged in Counts Three through Seven, the defendant THOMAS KENNEDY MCCORMICK shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to this offense, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 461(c). The United States will also seek a forfeiture money judgment against the defendant equal to the value of any property, real or personal, which constitutes or is derived from proceeds traceable to these offenses.

If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendant:

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

b. has been transferred or 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;

the defendant shall forfeit to the United States any other property of the defendant, up to the value of the property described above, pursuant to 21 U.S.C. § 853(p).

(Criminal Forfeiture, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Section 1963(a), Title 28, United Sates Code, Section 2461(c), and Title 21, United States Code, Section 853(p))

A TRUE BILL

_____
Foreperson

_____
JESSIE K. LIU
ATTORNEY OF THE UNITED STATES
IN AND FOR THE DISTRICT OF COLUMBIA