THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,	:	
Plaintiff,	:	
	:	
v.	:	**AFFIDAVIT IN SUPPORT OF**
	:	**CRIMINAL COMPLAINT**
MATJAZ SKORJANC,	:	**AND FORFEITURE AND**
a/k/a "iserdo,"	:	**APPLICATION FOR ARREST**
a/k/a "serdo,"	:	**WARRANTS**
FLORENCIO CARRO RUIZ,	:	
a/k/a "NeTK,"	:	
a/k/a "Netkairo,"	:	
MENTOR LENIQI,	:	
a/k/a "Iceman,"	:	
	:	
	:	
	:	
Defendants.	:	

I, Daniel S. Wierzbicki, a Special Agent at the Federal Bureau of Investigation of the United States Department of Justice, hereinafter referred to as the affiant, being duly sworn on oath, depose and state as follows:

I am a Special Agent of the Federal Bureau of Investigation (FBI) assigned to the Washington Field Office Criminal Computer Intrusion squad, and have been employed by the FBI since approximately March 2004. My training includes training in a wide variety of criminal matters and, specifically, computer crimes. As a Special Agent of the FBI, I am authorized to investigate crimes involving violations of federal law, including computer crimes. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer

crimes, computer evidence identification, computer evidence seizure and processing, and various criminal laws and procedures.

This affidavit is submitted in support of arrest warrants for MATJAZ SKORJANC a/k/a "iserdo," a/k/a "serdo," FLORENCIO CARRO RUIZ a/k/a "NeTK," a/k/a "Netkairo," and MENTOR LENIQI a/k/a "Iceman," for violations of federal law including violations of Title 18, United States Code, Section 1962(d) (Racketeering Conspiracy); Title 18, United States Code, Section 1349 (Conspiracy to commit wire fraud and bank fraud) Title 18, United States Code, Section 371 (Conspiracy to commit computer crimes, access device fraud, and extortion); and Title 18, United States Code, Section 1030(a)(5)(A) (Fraud and related activity in connection with computers).

It is respectfully requested that warrants issue for:

MATJAZ SKORJANC a/k/a "iserdo," a/k/a "serdo," date of birth July 30, 1986, resides in Maribor, Slovenia.

FLORENCIO CARRO RUIZ a/k/a "NeTK," a/k/a "Netkairo," date of birth October 28, 1978, resides in Zalla, Vizcaya, Spain.

MENTOR LENIQI a/k/a "Iceman," date of birth February 13, 1984, resides in Gorisnica, Slovenia

GENERAL ALLEGATIONS AND DEFINITIONS

At all times relevant to this complaint, unless otherwise alleged:

1. 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.

2. A "bot" is a software program that acts as an agent for a user. For example, crawler bots are programs used for searching the Internet. 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, 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 PC 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.

3. 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 through the use of 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."

4. Botnets are used in furtherance of a variety of criminal conduct, including, for example, (1) the launching of denial of service attacks 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.

5. 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.

6. A "POST Data Grabber" is a spyware tool that captures information entered into Internet-based forms by a computer user. A POST Data Grabber is capable of stealing a wide range of sensitive information, including website login credentials.

7. "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.

8. A "domain" is a set of subjects and objects on the Internet which 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.

9. "Exe" is short for "executable" or ".exe" or executable file, and refers to a binary file containing a program that is ready to be executed or run by a computer. Hackers many times refer to their malicious programs or code as ".exe" or "exe." For example, Hacker1 may ask Hacker2, "Did your exe spread over the network?"

10. An "exploit" is computer code written to take advantage of a vulnerability or security weakness in a computer system or software.

11. 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., 121.56.97.178). 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.

12. Internet Relay Chat ("IRC") is a network of computers connected through the Internet that allows users to communicate with others in real-time text (known as chat). IRC users utilize specialized client software to use the service and can access a "channel" which is administered by one or more "operators" or "ops." IRC channels are sometimes dedicated to a topic and are identified by a pound sign and a description of the topic such as "#miamidolphins." IRC channels are also used to control botnets that are used to launch DDOS attacks, send unsolicited commercial email, and generate advertising affiliate income.

13. Internet Relay Chat Daemon ("IReD") is a computer program used to create an IRC server on which people can chat with each other via the Internet.

14. 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."

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

16. "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.

COUNT ONE

(Title 18 United States Code, Section 1962 (d))

The Racketeering Conspiracy

17. Paragraphs 1-16 are herby incorporated and re-alleged herein.

18. From on or about September 29, 2008, and continuing up to in or about July 2010, in the District of Columbia and elsewhere, including Spain and Slovenia, the defendants MATJAZ SKORJANC a/k/a "iserdo," a/k/a "serdo," FLORENCIO CARRO RUIZ a/k/a "NeTK," a/k/a "Netkairo," and MENTOR LENIQI, a/k/a "Iceman," together with other persons known and unknown, being persons associated with a criminal enterprise controlled through an invitation-only, online forum known as "Darkode," 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 that enterprise through a pattern of racketeering activity involving multiple acts indictable under:

a. 18 U.S.C. § 1951 (extortion);

b. 18 U.S.C. § 1343 (wire fraud),

c. 18 U.S.C. § 1344 (bank fraud), and

d. 18 U.S.C. § 1029(a)(3) (access device fraud).

19. It was a further 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.

THE ENTERPRISE

20. MATJAZ SKORJANC a/k/a "iserdo," a/k/a "serdo," FLORENCIO CARRO RUIZ a/k/a "NeTK," a/k/a "Netkairo," and MENTOR LENIQI, a/k/a "Iceman were members and associates of a criminal enterprise. This criminal enterprise 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.

21. The Enterprise which operated in the District of Columbia and elsewhere in the United States, and in the countries of Slovenia and Spain, and elsewhere, operated through groups of individuals responsible for the various fraudulent schemes and criminal activities conducted by the Enterprise. While the overall structure and model of the Enterprise remained constant, the groups' and 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 defendant and others organized a forum, known as "Darkode," to facilitate the exchange of ideas, knowledge, and advice, and to provide a tightly controlled marketplace for buyers and sellers engaged in criminal activity.

22. Darkode's home page is located at http://darkode.com. Until recently, Darkode promoted itself as the "Best Malware Marketplace on the Net." It is comprised primarily of users interested in the use, sale, and deployment of malware for the purpose of generating revenue. It is run by an administrator, who from at least 2008 until approximately March, 2010, was SKORJANC. Members of Darkode are carefully vetted through a two step process. First, a prospective member must be invited to the forum by an existing member. Next, the prospective member must post an introduction on the Darkode forum, which typically includes the types of criminal activity in which the new user is seeking to engage. Only if existing members vouch for the new member is the new member allowed full access to the Darkode forum.

PURPOSE OF THE ENTERPRISE

23. The principal purpose of the Enterprise was to generate money for its members and associates. This purpose was implemented by members and associates the Enterprise through the commission of various criminal acts including: wire fraud, bank fraud, access device fraud, extortion and money laundering. I incorporate and re-allege paragraphs 29 - 113 herein.

24. The members and associates of the Enterprise sought, among other things, to:

a. 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

b. Promote and enhance the criminal activities of the Enterprise and its members and associates.

25. The Enterprise was bound together by, among other things, the members' and associates' common interest, knowledge, and usage of the Internet and its 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 owners through DDOS attacks, and to sell access to compromised computers to other forum members seeking to install their own malicious programs.

COUNT TWO

Conspiracy

(Title 18, United States Code, Section 1349)

26. From in or about September 29, 2008, and continuing up to in or about July 2010, in the District of Columbia, and elsewhere, including Spain and Slovenia, incorporating and re-alleging paragraphs 1-16 and 29-113 herein, the defendants, MATJAZ SKORJANC, a/k/a "iserdo," a/k/a "serdo," FLORENCIO CARRO RUIZ, a/k/a "NeTK," MENTOR LENIQI, a/k/a "Iceman," and others known and unknown, did knowingly and willfully conspire, combine, confederate and agree among each other and with other persons to:

a. devise a scheme and artifice to defraud and to obtain money and property from individuals and corporations 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. 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.

COUNT THREE

Conspiracy

(Title 18, United States Code, Section 371)

27. From on or about September 29, 2008, and continuing up to in or about July 2010, in the District of Columbia, and elsewhere, including Spain and Slovenia, incorporating and re-alleging paragraphs 1-16 and 29-113 herein, the defendants, MATJAZ SKORJANC, a/k/a "iserdo," a/k/a "serdo," FLORENCIO CARRO RUIZ, a/k/a "NeTK," MENTOR LENIQI, a/k/a "Iceman," and others known and unknown did knowingly and willfully conspire, combine, confederate and agree among each other and with other persons to:

a. knowingly cause the transmission of a program, information, code and command and as a result of such conduct, intentionally cause damage without authorization to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(a);

b. knowingly and with intent to defraud possess fifteen or more unauthorized access devices in violation of Title 18, United States Code, Section 1029(a)(3); and

c. did knowingly and intentionally obstruct, delay and affect, and attempt to obstruct, delay and affect, commerce as that term is defined in 18 U.S.C. § 1951, and the movement of articles and commodities in such commerce, by extortion as that term is defined in 18 U.S.C. § 1951 in violation of Title 18, United States Code, Section 1951.

COUNT FOUR

Damage to Protected Computer

(Title 18, United States Code, Section 1030(a)(5)(a))

28. From on or about September 29, 2008, and continuing up to in or about July 2010, in the District of Columbia, and elsewhere, including Spain and Slovenia, incorporating and re-alleging paragraphs 1-16 and 29-113 herein, the defendants, MATJAZ SKORJANC, a/k/a "iserdo," a/k/a "serdo," FLORENCIO CARRO RUIZ,a/k/a "NetK," MENTOR LENIQI, a/k/a "Iceman," and others known and unknown, knowingly caused the transmission of a program, information, code and command and as a result of such conduct, intentionally caused damage without authorization to a protected computer.

THE BUTTERFLY BOT AND MATJAZ SKORJANC

29. SKORJANC first came to the FBI's attention in or about October 2008. Username d01aR stated that he knew an individual by the username iserdo@gmail.com that could develop bots. In approximately October 2008 (all dates herein are approximate), Agents conducted searches on publicly accessible Internet sites for information about "iserdo@gmail.com," and discovered that iserdo@gmail.com is known by the screen moniker iserdo. It was learned that iserdo communicates via email or Google Talk with his Gmail account iserdo@gmail.com. A posting dated October 28, 2008, by "iserdo," on www.unk.bz, advertised for sale the BFBOT bot software. The posting listed the contact person as "iserdo@gmail.com," described the capabilities of the BFBOT software, and listed the basic

price as 350 Euros if payment was made by Western Union or "moneybrokers." The posting 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).

30. Beginning in October 28-30, 2008, the individual acting undercover on behalf of the FBI (a confidential human source, hereinafter CHS) initiated contact with SKORJANC by contacting him via Google Talk and email, through the account "iserdo@gmail.com," about the BFBOT. In those initial Google Talk and email communications, the CHS inquired about the purchase of the BFBOT from SKORJANC.

31. From 2008 to 2010, at the request of the FBI, the CHS had multiple online conversations with SKORJANC in which they discussed the features of the BFBOT and another form of botnet software known as ButterFly Flooder or "BFF." BFF was described as SKORJANC's newest product that was modular in nature, allowing customers to pick and choose the specific capabilities of the botnet software they desired. The CHS also helped to arrange FBI undercover purchases of the BFBOT and BFF malware from SKORJANC. The CHS learned from SKORJANC that the BFBOT software included the ability to spread to victim computers via Universal Serial Bus (USB) (a port used to connect external devices, such as printers and portable storage devices, to a personal computer), Microsoft Instant Messenger (MSN) (software that permits users to chat in real time with other MSN users) and Peer-to-Peer (P2P) (software designed to facilitate the transfer of data between computers, commonly used to

trade music and video files). According to SKORJANC, the BFBOT is able to infect any version of Microsoft Instant Messenger (MSN) and is capable of altering the text entered into MSN. BFBOT replaces the text entered by the user with a link to a website that, when clicked, results in the download of malware to the receiving system. SKORJANC further stated that the BFBOT was undetectable at novirusthanks.org, a website that permits the public to scan a given file with a number of different antivirus products. Certain versions of SKORJANC'S software had DDOS functionality.

32. In late 2009, the FBI obtained the contents of SKORJANC's email account, iserdo@gmail.com, via a federal search warrant. The means by which the BFBOT was capable of spreading itself to other, uninfected computers were detailed in an email SKORJANC to admin@1337crew.info. The email stated that the USB, MSN, and P2P infection methods were available in various versions of BFBOT, including: BFBOT LITE (250 EUR), BFBOT LITE ATTACKER (300 EUR), BFBOT STANDARD (350 EUR), and BFBOT STANDARD ATTACKER (400 EUR).

33. Additional features of the BFBOT were described in an email sent by SKORJANC to wg.fatal@gmail.com on December 2, 2008. In the email, SKORJANC indicates that the software includes DDOS features as well as the capability to steal sensitive information, including usernames and passwords, from users of the Firefox and Internet Explorer web browsers.

34. SKORJANC also authored and advertised other software such as DCI Bot, DownTroj, and Aspergillus. In an email dated December 8, 2007, SKORJANC emailed gov.hack@gmail.com with a list of DownTroj features, including the ability to remotely log keystrokes, remotely reboot or shut down a system, upload and download files, or install into a

location that is impossible to access with Windows Explorer. SKORJANC also stated that DownTroj included "more victims at the same time."

35. SKORJANC advertised his malware on various web sites such as http://www.unk.bz, http://darkode.com, and http://www.bfsystems.net. SKORJANC actively sought new opportunities to advertise his malware. For example, in email correspondence between SKORJANC and admin@1337crew.info on February 15 and 16, 2009, SKORJANC obtained access from admin@1337crew.info to a German underground forum located at 1337-crew.to/smf so that SKORJANC could market BFBOT to German speaking buyers.

36. On July 16, 2010, in Maribor, Slovenia, a confederate of SKORJANC positively identified the user of the email address iserdo@gmail.com as MATJAZ SKORJANC. This uncharged co-conspirator and SKORJANC are university classmates. SKORJANC enlisted the uncharged co-conspirator's assistance in updating the programming code for the existing BFBOT Graphical User Interface (GUI). The uncharged co-conspirator also assisted SKORJANC in creating a web site related to the BFBOT. The uncharged co-conspirator used email address jernej_5@hotmail.com to communicate with SKORJANC (who used iserdo@gmail.com), where they discussed development of the BFBOT GUI. Agents also showed the uncharged co-conspirator a photograph of MATJAZ SKORJANC a/k/a "iserdo," a/k/a "serdo." The uncharged co-conspirator identified the person in the photograph as iserdo.

37. On February 28, 2008 an email was sent from iserdo@gmail.com to iserdo@gmail.com that included an attachment named "images.rar" that contained fifty (50) screenshots of what appears to be a school exam. At the top of each image the name of the test taker, "Skorjanc Matjaz," appears.

38. Analysis of SKORJANC's email account showed that SKORJANC followed a pattern of selling customized versions of BFBOT to individuals around the world. Many of the buyers requested customized features to be included in their version of the BFBOT. After coordinating the specific requirements for the BFBOT with SKORJANC, the buyers often sent payment via Liberty Reserve or Western Union. SKORJANC instructed that payments be sent to an uncharged co-conspirator who resided at his address, known hereafter as "NC." One of the specific requirements for purchasing the BFBOT was to provide SKORJANC with a list of domain names and update codes. The domain names and codes were then programmed by SKORJANC into the customer's specific version of the BFBOT. Once SKORJANC received the payment, domain names, and codes, SKORJANC sent a password-protected file (usually named something similar to bfbot.rar or boat.rar) to the buyer and then advised the buyer to chat with him on MSN Messenger to obtain the password to the .rar file.

39. Analysis of the iserdo@gmail.com email account revealed multiple instances of SKORJANC directing BFBOT buyers to send Western Union payments to NC in the city of Maribor, Slovenia. For example, in an e-mail dated July 5, 2009, which contained a chat log transcript, schlist90210@gmail.com (Schlist) and SKORJANC discussed payment for BFBOT. SKORJANC stated to Schlist that he would receive the BFBOT as soon as possible after sending the money, and that the Western Union payment should be made to NC in MARIBOR, SLOVENIA.

40. Records obtained from Western Union show that on or about July 9, 2009, a Western Union payment was sent from an uncharged co-conspirator in Romania to NC in the amount of 1002.89 Euro. On the same date, Schlist sent iserdo@gmail.com a list of domains and codes for his version of BFBOT.

41. In August and September of 2009, SKORJANC and Schlist again communicated via email, with Schlist providing the domain names hnox.org, socksa.com, ronpc.net and other configuration information for "bfbot pro"/"bfbot." Schlist requested that SKORJANC include the three domains within his customized version of BFBOT. Schlist complemented SKORJANC on the stability and speed of the BFBOT and stated that BFBOT was well worth the money.

42. On May 13, 2009 and September 27, 2009, waisted.time@hotmail.com corresponded via email with SKORJANC. The subject of these emails was "My BFBOT Pro Lite Config" and "new and old dns." Waisted.time@hotmail.com provided SKORJANC with domain names and codes. A Western Union payment made by the uncharged co-conspirator who owns waisted.time@hotmail.com to NC on May 13, 2009 corresponds to the email communication of May 12, 2009 in which the uncharged co-conspirator provided SKORJANC with domain names.

43. The owner of the email address waisted.time@hotmail.com was interviewed by the FBI, and stated that he purchased BFBOT from iserdo and that he was involved in procuring "installs."

44. There were at least twenty other individuals that sent money to NC who also communicated via email with SKORJANC. Some of these email conversations included the customer providing SKORJANC with first and last names, Western Union transaction numbers, payment amounts matching money sent to NC, BFBOT domain names, and update codes. The conversations followed a similar pattern relating to the purchase of the BFBOT.

45. Western Union records reveal that at least 180 Western Union payments were sent to NC from individuals in at least 36 different countries.

THE MARIPOSA BOTNET

46. In May, 2009, a fast-spreading botnet was observed by the IT security company Defence Intelligence, Inc. Defence Intelligence named this botnet "Mariposa," the Spanish word for butterfly. Based upon the facts set forth below and other information, it has been determined that the Mariposa bot is a customized version of Butterfly Bot (BFBOT) written by SKORJANC and deployed by RUIZ. Industry reports indicate that the Mariposa bot infected at least 2.6 million computers worldwide, and rank it one of the largest botnets ever created.

47. Between October 2008 and May 2009, Ruiz, using the email address netkairo@hotmail.com, communicated with SKORJANC at iserdo@gmail.com regarding purchase, delivery, and configuration of BFBOT. On October 22, 2008, SKORJANC sent an email to RUIZ requesting configuration information for BFBOT. Between October 23, 2008 and December 29, 2008, SKORJANC sent three emails to RUIZ. These emails contained attachments named as follows: bfbv1.0.rar, bfv1.2.rar, bf-netkairo.rar. These attachments were named consistently with different versions of BFBOT. Between February 20, 2009 and May 9, 2009, RUIZ sent three emails to SKORJANC specifying domain name servers to be incorporated into RUIZ's customized version of BFBOT.

48. On April 29, 2009, RUIZ made a Western Union payment of 400 Euros to NC in Maribor, Slovenia. This payment directly matches email correspondence between netkairo@hotmail.com and iserdo@gmail.com on April 29, 2009, where RUIZ provided various BFBOT parameters to SKORJANC. On August 11, 2009, made another Western Union payment of €500 to NC in Maribor, Slovenia.

49. RUIZ used a customized version of the BFBOT to collect Internet login credentials and credit card information. The BFBOT gathered this information in multiple ways.

A search of RUIZ's residence at the time of his arrest in February 2010 yielded a Universal Serial Bus (USB) flash memory drive that was used by RUIZ to store numerous log files generated by the BFBOT. User manuals associated with multiple versions of BFBOT were also found on RUIZ's memory drive. These manuals describe that BFBOT is designed to spread surreptitiously to victim computers and collect usernames and passwords from Internet browser files. These documents further describe BFBOT as capable of executing a DDOS attack, and installing additional malware on victim computers. These documents credit "iserdo" as the developer of BFBOT and include iserdo@gmail.com as a method of contact.

50. Butterfly Bot source code was also located on RUIZ's flash memory drive. The source code files indicate "Copyright (c) 2008 by iserdo" in the file header. In addition to these documents, a copy of the malware file, bf-netkairo.rar, sent to RUIZ at netkairo@hotmail.com from SKORJANC at iserdo@gmail.com, on December 29, 2008 was located on RUIZ's flash memory drive. The version sent via email and the version located on RUIZ's flash memory drive were determined to be identical through the use of digital fingerprinting tools regularly used to identify and analyze malware.

51. The BFBOT generates various log files that record the spread of the malware to victim computers, as well as the theft of Internet credentials and credit card information. An analysis of RUIZ's flash memory drive revealed that RUIZ stored numerous log files generated by the BFBOT. The log files are generated automatically and stored in folders also containing BFBOT malware. The folders containing the log files have names associated with BFBOT, such as "bf" or "bf1.29." The log files show the computer compromised as well as the specific username/password or credit card information stolen. In total, log files found on RUIZ's flash memory drive contain over 522,000 username/password pairs and approximately 217 instances

of credit card information. Based upon my experience, collecting this information is often an important step in various schemes to fraudulently obtain money, services and property from unwitting victims, including individuals, merchant and financial institutions. For example, the credit card information could be used in a scheme to obtain or attempt to obtain property in that individuals misrepresent themselves as the legitimate account holders, when they are not, and thereafter obtain money, services or property using the account.

52. In late February 2010, Spanish authorities arrested RUIZ along with two additional individuals, known hereafter by their aliases Ostiator and Weke, who were working with RUIZ to control the Mariposa botnet. Weke aided in the spread of the malware to grow the botnet. Furthermore, Weke paid SKORJANC for malware, and acted as an intermediary to provide DDOS services to clients through the use of the Mariposa Botnet. Ostiator shared administration responsibilities for the Mariposa Botnet with RUIZ. RUIZ participated in DDOS attacks and extortion through the use of DDOS attacks as well as collecting and trading online credentials and credit card information.

53. RUIZ used the Mariposa Botnet to execute a DDOS attack against website www.telegrow.com for the purpose of extortion. According to chat logs obtained during the search of RUIZ's residence and analyzed by the Spanish Guardia Civil, the administrators of www.telegrow.com were successfully extorted for 1,000 Euro. According to the Spanish Guardia Civil, the purpose of the attack was to request an amount of money in lieu of stopping the attack.

54. An individual known by the alias "Torbe" contacted RUIZ and Ostiator to request that they execute a DDOS attack against Torbe's business competition. Chat logs obtained during the search of RUIZ's residence, and analyzed by the Spanish Guardia Civil, demonstrate that RUIZ and Ostiator intentionally executed a DDOS attack against several websites at the

request of Torbe. Among those websites attacked are www.irinavega.com, www.xnet.es, www.xcanal.es, and www.grupoifg.com. Torbe paid RUIZ and his associates for this service.

55. According to information collected by an Internet industry working group, over ten million unique Internet Protocol (IP) addresses are known to have been compromised by the Mariposa Botnet. At least 2.6 million IP addresses were known to have been simultaneously infected. Among these, over 400,000 IP addresses have been identified as belonging to hosts within the United States. Approximately 5,700 IP addresses are registered to entities in Washington, DC. Six of those IP addresses within are registered to United States Government entities within the District of Columbia. The actual size and spread of the Mariposa Botnet may have been much larger.

56. The FBI reviewed forum postings on darkode.com obtained by a CHS that relate to RUIZ (using the moniker NeTK) and the Mariposa Botnet. The postings state that the Mariposa Botnet had "google hijack functionality." In February 2010, an FBI CHS communicated covertly with SKORJANC and discussed the Mariposa Botnet. SKORJANC stated:

> 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."

The CHS asked SKORJANC if the CHS could purchase Mariposa, and SKORJANC stated:

> as for this google thingie, im not selling, you would have to offer really good money to get it :), of course, all works with bff [ButterFly Flooder]."

The CHS then asked how much SKORJANC would charge for the "connect hook + post data grabber" and Iserdo stated,

> ch is 200 eur, pdg is 200 eur, if you buy them together its 300 eur, read here about bff modules: http://darkode.com/viewtopic.php?t=2381&start=0."

In this conversation, I understand "ch" to mean Connect Hook and "pdg" to mean "post data grabber," a password stealing tool. Finally, the CHS asked Iserdo about including MSN spreader functionality (which would allow the bot to spread via MSN Messenger) in the ButterFly Bot, and SKORJANC stated:

msn spreader, usb, basic flooder and visit are free modules.

57. RUIZ also profited by selling access to the compromised computers that were part of his Mariposa Botnet. The access consisted of uploading and installing malicious software provided by other individuals onto the previously compromised computers of his botnet for a price. Known as "installs," the installation of additional malicious software was negotiated on a price per computer.

58. RUIZ advertized the sale of installs on the Darkode forum. For example, on December 17, 2009, an individual with the moniker _0x90u started a forum thread asking if anyone on the forum was willing to sell installs for his malware. RUIZ, using his moniker NeTK, responded to his post on December 18, 2009 by posting "33k mix if u want pm me." Based on my training and experience, I understand RUIZ's reply to mean that he had a botnet consisting of 33,000 previously compromised computers that were located all around the world and that if the potential buyer was interested in purchasing access to install his software, he could reach RUIZ by private message via the Darkode forum.

59. On December 19, 2009, an FBI Undercover Employee (hereinafter "UC-1") sent RUIZ a private message on Darkode asking if he had installs for sale. UC-1 provided RUIZ with an email address associated with an MSN Messenger online instant messaging account and asked for RUIZ to contact UC-1.

60. On January 8, 2010, RUIZ, using the email address hamlet1917@hotmail.com and the moniker "NeTK," contacted UC-1 via MSN Instant Messenger. In the online conversation, RUIZ sold access to his botnet for the purpose of installing malware on the compromised computers RUIZ controlled. RUIZ's charged UC-1 $240 for 8,000 installs. UC-1 and RUIZ agreed to use ePassporte, an online payment service, as the method of payment. RUIZ instructed UC-1 to send payment to the ePassport account "florenciocarro." UC-1 sent payment of $240 to RUIZ via ePasspoarte that same day.

61. RUIZ asked UC-1 for the executable program to install onto the previously compromised computers of his botnet. RUIZ was provided an executable program, developed by the FBI, to be uploaded to the computers of the botnet. The executable program reports the IP address of the infected computers back to the FBI for the purpose of identifying victims, but takes no other action. After providing RUIZ with the executable program, RUIZ told UC-1 that he was going to start the installation. Between January 8, 2010 and January 9, 2010, the executable program provided to RUIZ was installed on over 13,000 previously compromised computers located worldwide.

62. Information from ePassporte showed that the subscriber for the "florenciocarro" account was Florencio Carro, residing at AV Lanzagorta 3 4b, Zalla, Spain. On January 8, 2010, login activity showed that IP address 85.84.80.164 accessed this account. This IP address resolves to a computer located in Spain. This ePassporte account was associated with the email address floxter@hotmail.com.

63. Information obtained from Microsoft shows that the email address hamlet1917@hotmail.com was accessed from IP address 85.84.80.164 on January 9, 2010. As stated previously, this IP address resolves to a computer located in Spain.

64. On February 3, 2010, a search warrant was conducted at the residence of FLORENCIO CARRO RUIZ located at Calle La Calzada 5 1 D 48800 in the locality of Viscaya, by the Spanish Guardia Civil. In connection with the search warrant, several digital items were seized. One of the items seized was a Macintosh computer. A review of the contents of the seized evidence showed that the MSN Messenger account associated with hamlet1917@hotmail.com was accessed from that computer. In addition, an MSN Messenger account associated with floxter@hotmail.com was accessed from the seized computer.

65. According to the Spanish Guardia Civil, another computer seized in the search warrant contained a file in the computer's Internet Explorer Cache that associated the computer to the IP address 85.84.80.164.

ICEMAN – MENTOR LENIQI

66. On or about April 15, 2010, an individual with the moniker "Iceman" posted a thread on Darkode advertising the sale of servers that were compromised. As part of the server compromise, administrative access, or "root" access, to the servers was gained. An individual with root access has the ability to take full control of the server. With full control, the server can be used to conduct further illegal activity including hosting the command and control of a botnet, running a website that distributes malicious programs, or distributing trademarked software.

67. In response to Iceman's posting, UC-1 contacted Iceman on Darkode and communicated his desire to purchase root access to the servers. UC-1 provided Iceman with an email address associated with a MSN Messenger online instant messaging account and asked for Iceman to contact UC-1.

68. On April 15, 2010, Iceman contacted UC-1 via MSN Messenger and identified by the email account ice@iceman.in. UC-1 was communicating from a computer that was connected to a proxy server located within the District of Columbia. As a result, all Internet traffic to and from UC-1's computer was being filtered though the proxy server. In the conversation, Iceman stated that he had root access to several servers. Iceman further explained that the compromised servers were located in different datacenters and located in the United States, Europe, Russia, and China. Iceman further provided that he gained access to the servers by scanning for vulnerable servers. Once he gained access to the servers, he did not change the passwords.

69. Iceman negotiated the sale of thirteen servers for which he had root access to UC-1 for $60. Iceman sent UC-1 a file named "shits.txt" that contained the IP addresses of the compromised servers along with the password. The list provided the IP addresses and passwords for fifteen servers, eleven of which were located within the United States. UC-1 and Iceman agreed to use PayPal, an online payment service, as the method of payment. Iceman instructed UC-1 to send payment to the PayPal account identified by the email address leniqi.mentor@siol.net. UC-1 sent payment of $60 to Iceman via PayPal that same day.

70. After the transaction, Iceman told UC-1 that he was located in the same city as Iserdo and that he had purchased the BFBOT from him. Iceman further provided that he had used the malicious software to make his own botnet.

71. Information from PayPal showed that the PayPal account associated with the email address leniqi.mentor@siol.net was subscribed by MENTOR LENIQI, residing at 32 Gorisnica, Maribor, Slovenia. On April 15, 2010, login activity showed that the IP address

109.182.12.244 accessed this account. This IP address resolves to a computer located in Slovenia.

72. On July 30, 2010, a search warrant was executed by the Slovenian National Police at the residence of MENTOR LENIQI ("LENIQI"), who resided at Gorisnica 32, Maribor, Slovenia. Several items of evidentiary value, including digital evidence, were collected. A review of a computer seized from LENIQI contained a file named "shits.txt." The file contained the IP address and password to thirteen of the fifteen servers provided to UC-1. The computer also contained a log of the chat conducted with UC-1.

73. Following the search of LENIQI's residence, LENIQI was contacted and consented to a voluntary interview with the Slovenian National Police at the Slovenian Criminal Police Offices in Maribor, Slovenia. LENIQI was not under arrest and agreed to have FBI Agents present during the interview. In the interview, LENIQI stated that he uses the online moniker "iceman" and the email address ice@iceman.in. LENIQI also stated that he uses the account ice@iceman.in for his ICQ and MSN Messenger accounts. LENIQI stated that he was a member of the Darkode forum and uses the name "iceman" on the forum.

74. LENIQI told the interviewing FBI Agents that he had sold root access to servers provided to him by a person known as "Buz." This individual operates an IRC-based botnet that is able to crack passwords on web hosting accounts and servers. The botnet scans for common web host interfaces, such as cPanel, and then attempts a brute force password attack on the servers. If successful, the IP address and cracked credentials are displayed in an IRC channel. LENIQI had access to this IRC channel and this is how he obtained the credentials for the accounts that he sold. LENIQI also stated that he sold access to compromised servers to other Darkode members.

75. LENIQI also told the interviewing agents that he had purchased the Butterfly Flooder Bot from SKORJANC. LENIQI stated that he was introduced to SKORJANC by an individual who had purchased the bot to conduct DDOS attacks. LENIQI then contacted SKORJANC at the email address, iserdo@gmail.com. LENIQI contacted SKORJANC through this account and arranged to purchase a copy of the bot for 400 Euro.

76. In the review of the search warrant results for the email account iserdo@gmail.com on October 29, 2009, an email was located that originated from email address icemangjk@hotmail.com. In the email, LENIQI provided SKORJANC the information necessary to customize LENIQI's copy of the BFBOT, including three domain names that LENIQI would use to administer the bot, along with other technical information requested by SKORJANC.

77. A search of a computer seized by the Slovenian National Police revealed a file named info.txt that contained the same information provided in the email by LENIQI to SKORJANC. Located on the same computer, a Butterfly Bot folder was found. Inside of the folder, several log files were found. The first log file, named chan_0.log, showed victim compromised computers joining and quitting a command and control server. A file named chan_1.log showed victim computers that were running the USB spreading capabilities of the Butterfly Bot. A file named chan_2.log showed victim computers spreading the bot via MSN Messenger spreading. A file named chan_3.log showed victim computers downloading, via peer to peer, a file named "amgelina-porn-video-downalod.exe." A file named chan_4.log showed the infected drives for each of the victim computers. A file named chan_5.log showed a server being attacked by a Distributed Denial of Service attack. A file named chan_6.log showed data collected from the web browsers of victim computers. The data collected included username and

passwords from form data. A file named chan_7.log appeared to contain the IP addresses of compromised victim computers that could be operated remotely.

78. Also present in the Butterfly Bot folder was a user manual indicating that the software possessed by LENIQI was version 1.51 of ButterFly Bot PROFESSIONAL. A file named settings.ini showed that LENIQI's bots were connecting to a command and control server identified by the IP address 91.185.206.186. This IP address resolves to a server located in Slovenia and according to the publically available web site www.centralops.net, this IP address is registered to LENIQI, GORISNICA 32A, SLOVENIA. Moreover, the domain associated with the above-referenced IP address is webmail.ngulesh.info. This domain is one of the domains provided by LENIQI to SKORJANC upon purchasing the Butterfly Bot on October 29, 2009.

79. The digital evidence seized by the Slovenian National Police also contained saved online chat logs. On January 7, 2010, LENIQI conducted an online chat with RUIZ, contacting RUIZ using the MSN Messenger account associated with hamlet1917@hotmail.com. In the chat, LENIQI asked RUIZ to install malicious software onto 5,000 previously compromised computers. LENIQI told RUIZ that he needed RUIZ to upload and install the Butterfly Flooder Bot that was to be provided by SKORJANC. LENIQI then asks RUIZ if he knows of a command on the Butterfly Flooder Bot that would conduct a Distributed Denial of Service attack that would run silently on a server. RUIZ then responded back to LENIQI with a Butterfly Flooder command that would perform a silent DDOS attack.

80. On January 9, 2010, LENIQI asked RUIZ if the Butterfly Flooder Bot has a strong DDOS attack. RUIZ responded that the bot does have a strong attack.

81. On December 29, 2009, LENIQI conducted an online chat conversation with SKORJANC, identified by the email address iserdo@gmail.com. In the chat, LENIQI tells

SKORJANC that he is interested in purchasing the Butterfly Flooder Bot. LENIQI expressed the need for the Butterfly Flooder Bot to have good Distributed Denial of Service Attack capabilities. SKORJANC replied that the bot "has a good attack" and was "the best." SKORJANC then explained to LENIQI how best to conduct a DDOS attack using the "TCP flooding capabilities" of the Butterfly Flooder bot.

82. The Slovenian National Police provided the FBI with the contents of a chat that occurred between SKORJANC and LENIQI on January 11, 2010. In this chat SKORJANC and LENIQI negotiated the purchase of the ButterFly Flooder Bot for 500 Euro. SKORJANC then instructed LENIQI to send the funds to a bank account located in Maribor, Slovenia. LENIQI asked SKORJANC to explain the post data grabber module for the Butterfly Flooder Bot, a conversation captured in the following chat transcript:

(8:33 PM) iceman: iserdo can you say what specification has post data grabber and how much it costs?
(8:34 PM) iserdo: 200 eur
(8:34 PM) iserdo: draws in all post data from IE6,7,8
(8:34 PM) iserdo: HTTP and HTTPs
(8:34 PM) iserdo: for stealing info
(8:34 PM) iserdo: logins
(8:34 PM) iserdo: paypal, etc
(8:34 PM) iserdo: banks
(8:34 PM) iceman: huh
(8:34 PM) iceman: this is neat
(8:35 PM) iceman: similar to I6 I7 If but I6 I7 If are bad they have very little logins, etc
(8:35 PM) iceman: hmm, it's too much if i get this as well
(8:35 PM) iceman: 700 eur phew
(8:39 PM) iceman: is it possible to get it together with post data grabber for 600 eur?
(8:40 PM) iserdo: nope, it won't work
(8:41 PM) iserdo: but the thing is much better than explorer pass grabber :)
(8:41 PM) iserdo: cause here you'll have catchal pass regardless if it's saved or not :P
(8:41 PM) iserdo: in any case
(8:41 PM) iserdo: problem can be only with some banks that have tokens :)
(8:41 PM) iserdo: that are valid for only a few seconds

Based on my training and experience, I understand SKORJANC to be explaining to LENIQI that the post data grabber collects the "POST data" from Microsoft Internet Explorer versions 6, 7, and 8. The post data is information that is submitted to a website after a user fills out a web-based form. SKORJANC notes that the post data grabber can be used to steal sensitive login information, such as usernames and passwords, from financial websites.

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

84. On February 16, 2010, LENIQI told SKORJANC that he had bank wire transferred the remaining funds to SKORJANC. SKORJANC then instructed LENIQI to provide him the unique identifier for his computer and to send him three domains to the email address iserdo@gmail.com. LENIQI replied to SKORJANC that he had sent him the required email.

85. On July 15, 2010, SKORJANC and NC were arrested by Slovenian authorities on Slovenian charges in Maribor, Slovenia. Both were released after they were arrested. Slovenian authorities have confirmed that SKORJANC is the real identity of Iserdo.

THE DARKODE ENTERPRISE

86. The email string below illustrates that membership for Darkode is by invitation only. . In the string, SKORJANC – using his alias "Iserdo" – identifies himself as "The Management" of darkode.com, and provides a new user with instruction on how to access Darkode:

> From: iserdo@gmail.com <iserdo@gmail.com>
> Subject: Welcome to darkode.com Forums
> To: XXXXXXXXXXX

Date: Sunday, November 9, 2008, 5:11 PM

Welcome to darkode.com Forums

Please keep this email for your records. Your account information is as follows:

Username: XXXXXXXXXX
Password: XXXXXXXXXX

Your account is currently inactive. You cannot use it until you visit the Following link:

http://forums.darkode.com/profile.php?mode=activate&u=XXXXXXXXXXXXXXX

Please do not forget your password as it has been encrypted in our database and we cannot retrieve it for you.
However, should you forget your password you can request a new one which will be activated in the same way as this account.

Thank you for registering.
--
Thanks, The Management

87. When the user responds that his password doesn't work, SKORJANC informs him that his account has been deleted due to inactivity. The user then asks how he can regain access to the forum. SKORJANC responds as follows:

From: Serdo Muro <iserdo@gmail.com>
Subject: Re: Welcome to darkode.com Forums
To: XXXXXXXXXXXX
Date: Tuesday, February 10, 2009, 6:48 PM

someone has to invite you again. whoever invited you, ask him to invite you again.

88. As stated previously, the Darkode forum, which was administrated by SKORJANC, described itself as "The best malware marketplace on the net." The forum is a

self-contained market governed by rules and logic that closely mimic those of the legitimate business world, including expectation about its members' conduct and a system of stratification based on knowledge, skill, activities, and reputation. The forum also has an organized structure and hierarchy in which members are assigned a specific ranking based on experience and reputation, and new members undergo a screening or promotion process. Its members are networks of vetted individuals agreeing to cooperate for particular criminal operations. The members of the forum are have specialized occupations, primarily as coders, hackers, and vendors, to conduct specific criminal activity.

89. The Darkode forum is organized into the following hierarchical framework: administrators, who serve as the governing council; moderators, who oversee one or more subject matter specific forums on the site; and members, who use the site to gather and provide information about perpetrating criminal activity.

90. Members on the forum use their specialized occupations to facilitate and further the criminal activity of its other members. The activity is illustrated by a September 29, 2008 message thread initiated by SKORJANC entitled "p2p programs and their sharing folder." In the thread, SKORJANC seeks assistance from the members of Darkode in developing the capability of his botnet software to spread itself to other computers via Peer-to-Peer file sharing.

91. In his post, SKORJANC states:

> im too lazy to install all p2p programs and check how and where is their sharing folder defined. so i would please you to share your knowledge with me...all other p2p spreaders in other bots are peace of shit, cos they use static folder, not to mention their 'Program Files', which is of course named 'Program Files' only on english version of win."

92. Based on my training and experience, I understand SKORJANC's post to be seeking assistance from other Darkode members about the functionality of various Peer-to-Peer software programs. Because SKORJANC's botnet software attempts to spread itself through Peer-to-Peer file sharing, SKORJANC needs to know the mechanics of how various Peer-to-Peer file sharing programs function. In his message, SKORJANC disparages other software that attempts to spread through Peer-to-Peer as "shit" because its authors fail to account for the regional differences between different Windows-based computers, which limits the ability of these programs to propagate themselves. In response to SKORJANC's message, several members of the forum responded with advice and suggestions, including sample code that SKORJANC could use to improve his malware.

93. Another example of collaboration within Darkcode takes place on November 10, 2009, in a message thread entitled "coders making FUD injectors for BFF." SKORJANC posted under this topic the following:

> Im looking for coders, that like to deal with FUDness, UDness.polymorphism/ metamorphism. You would be making various injectors for BFF and sell them to BFF customers. You can make standard static kind of injectors or polymorph/metamorph ones. You name the price, you take payments directly from customers. I give you example code and specifications you need to follow to make BFF compatible injector. Btw: customers are highly interested in injectors that would be (F) UD for longer time than current crypters that can be purchased or even some good polymorphic methods etc…contact me if interested."

94. RUIZ responded to SKORJANC's post that he knew of individuals that had the knowledge to create such a product.

95. Based on my training and experience, I understand SKORJANC's message to be seeking assistance from Darkode members in creating a software product that would allow for the Butterfly Flooder Bot to be undetectable to antivirus software. In order for the Butterfly

Flooder Bot to function on a victim computer, the bot must not be detected and removed by antivirus software. Antivirus software detects malicious software by comparing the files on a computer to a database of known malicious programs. Through sophisticated programming techniques, coders can hide malicious software from antivirus detection by changing the malicious program's signature, thereby rendering the malicious software "UD" (undetectable to most antivirus products) or "FUD" (fully undetectable to all antivirus products.)

96. In his post, SKORJANC offers to provide the code that he designed in creating the bot and specifications that would allow for the add-on software to function. The members creating the add-on software would be allowed to market the product to other members who purchase the Butterfly Flooder Bot.

97. In a similar vein, on February 24, 2010, a Darkode member (hereafter "M1") posted a message on the forum under the topic "Best bot on the market?" In the post, M1 wrote:

> why don't we buy a private custom bot similar to BFF? We can determine the needs and hire a programmer to code it. All people who danotes (pays) the project gets the code. Coder makes the main base and it's plugin enabled. So each person can code his own plugins for their needs. If you don't want to use IM spreading, you don't install it on your bots. If you need ddos, you write your own custom plugin and load it to your victims. Coder continues to develop and improve the base only and send the updates (source) regularly to customers. I think if we combine a group here we can hire a good coder.

98. Based on my training and experience, M1 was suggesting the members of the forum hire an individual who specializes in software coding to create custom malware that has functions that are decided upon by the group. The custom malware would be designed to allow for specific function add-ons at a later date. Individuals who are part of the group would have the original source code of the malware. By combining the financial resources of the group, a coder could be hired to create this custom malware.

99. Another Darkode member (hereafter "M2") replied to M1's post: "closed source would be better I think unless the only customers are like a small group of partners :)." M2 suggested that the members of the group do not have access to the original source code.

100. Darkode member (hereafter "M3") replied to "count me in." M3 is agreeing in taking part in the project.

101. M1 then replied to M2 by writing:

> I just needed the source for future / If coder dies -> project dies. There maybe two options: 2 buyer group. 1st one just got binaries a pays X. 2nd one gets source and pays 2-3X. If coder dies 1st group members can buy the source from 2nd group members (just an idea). If people write their needs here we can try to determine the ~budget we need. The group must be small group of trusted members. People who has chance to leak the project shouldn't be accepted into the group.

102. Based on my training and experience, M1 is suggesting that there should be two different categories of code buyers. One category of members would be members who purchase only the executable program of the malware and not the source code that would allow the owner to freely replicate or change the program. The other category would be members who purchase the source code for a higher amount. A member of the first category can then pay an additional amount from members of the other category if they desire the source code in the future. M1 also suggested that the members of the group must be trusted.

103. M2 replied back to M1 by writing: "or just have a group working on it together some people can code and others can test/spread it and stuff, so even not technical ppl can contribute."

104. Based on my training and experience, M2 is suggesting that a group of individuals could design the custom malware. Individuals who lack the expertise in creating code would be

able to test the product created by the coders. In this way, individuals who lack the coding expertise could contribute.

105. This topic illustrates that the members of Darkode work closely together, using the specialized skills of each member, in order to further and facilitate the criminal activities of its members.

106. The members of Darkode also provide information and methods to each other in order to evade detection by law enforcement. On August 3, 2009, a Darkode member (hereafter "M4") posted to the topic "Instant messaging encryption." M4 wrote:

> 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.

107. Based on my training and experience, I understand M4 to be asking the members of Darkode to describe their methods of keeping law enforcement from intercepting and reading their online communications. In his message, M4 references using the program "SIMP" to encrypt the communication being transferred over the Internet. Open source research confirms that SIMP is a program capable of encrypting instant message traffic.

108. A Darkode member (hereafter "M5") replied to M4's post that he uses SIMP. However, M5 also stated that SIMP is not effective if the other person in the communication is not using the program.

109. Another Darkode member (hereafter "M6") wrote that he uses encryption in order to protect his MSN Messenger logs.

110. SKORJANC followed M6 post by writing:

> not keeping msn logs is more important. Without proof on your HD they have nothing.

111. In addition to facilitating the exchange of ideas, knowledge, and advice, Darkode also functions as a tightly controlled marketplace for buyers and sellers engaged in criminal activity. On June 27, 2010, a Darkode member (hereafter "M7") posted a message under the forum thread "BFBOT Pro 1.51." M7 wrote:

> 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 120$ today (discussable). Payment via LR/WMZ. 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."

112. Based on my training and experience, I understand M7's message to be advertizing the sale of a botnet consisting of 900 victim computers. The price of the botnet was $120 and payment was being accepted using various forms of online payment options. The victim computers were being controlled by a command and control server of which access was gained by hacking. M7 will sell the server for $90. The member purchasing this package would be able to use the capabilities of the malware to further their criminal activity.

113. The Darkode forum is a transnational criminal enterprise. Its structure, division of labor, support network, and its members' participation in various criminal activities in countries throughout the world facilitate the exchange of ideas, knowledge, and advice, and provide a tightly controlled marketplace for buyers and sellers engaged in criminal activity.

114. The facts and circumstances set forth in this affidavit demonstrate that there is probable cause to believe that MATJAZ SKORJANC a/k/a "iserdo," a/k/a "serdo," FLORENCIO CARRO RUIZ a/k/a "NeTK," a/k/a "Netkairo," and MENTOR LENIQI a/k/a

"Iceman," violated federal law including violations of Title 18, United States Code, Section 1962(d) (Racketeering Conspiracy); Title 18, United States Code, Section 1349 (Conspiracy to commit wire fraud and bank fraud) Title 18, United States Code, Section 371 (Conspiracy to commit computer crimes, access device fraud, and extortion); and Title 18, United States Code, Section 1030(a)(5)(A) (Fraud and related activity in connection with computers).

FORFEITURE ALLEGATIONS

Pursuant to Rule 32.2(a), Federal Rules of Criminal Procedure, notice is hereby given to the defendants that the United States will seek forfeiture as part of any sentence in accordance with Title 18, United States Code, Sections 1963 and 982, in the event of any defendant's conviction(s) under either Count 1, 2 3, or 4.

RACKETEERING FORFEITURE

1. Pursuant to Title 18, United States Code, Section 1963(a), each defendant who is convicted of the offense set forth in Count 1 of this Indictment shall forfeit to the United States the following property:

(a) Any interest acquired or maintained pursuant to Section 1962;

(b) Any interest in, security of, claim against, or property or contractual rights of any kind affording a source of influence over, the enterprise described in Count 1 which was established, operated, controlled and conducted pursuant to Title 18, United States Code, Section 1962;

(c) Any property constituting or derived from proceeds obtained directly and indirectly from racketeering activity pursuant to Title 18, United States Code, Section 1962;

(d) The property subject to forfeiture shall include, but not be limited to, the following:

i. A sum of money representing the total amount of proceeds obtained by defendants, as a result of their violation of Title 18, United States Code, Section 1962; and

ii. Property located at [redacted] Maribor, Slovenia [redacted] and storage room 42.E Land Register Number 1687/3 (Okrajno Sodisce v Maribor, Local Court Maribor).

2. If more than one defendant is convicted of Count 1, the defendants so convicted are jointly and severally liable for the amount subject to forfeiture under this paragraph.

All pursuant to Title 18, United States Code, Section 1963.

WIRE FRAUD FORFEITURE

1. Pursuant to the provisions of Title 28, United States Code, Section 2461 and Title 18, United States Code, Section 981(a)(1)(C),each defendant who is convicted of the offense set forth in Count 2 (Wire Fraud Conspiracy) shall forfeit to the United States the following property:

Any property constituting, or derived from, proceeds the defendants obtained as the result of such violation.

(a) The property subject to forfeiture shall include, but not be limited to, the following:

i. A sum of money representing the total amount of proceeds obtained by defendants, as a result of their violations of Title 18, United States Code, Section 1343; and

ii. Property located at [redacted] Maribor, Slovenia [redacted] and storage room 42.E Land Register Number 1687/3 (Okrajno Sodisce v Maribor, Local Court Maribor).

All pursuant to the provisions of Title 28, United States Code, Section 2461 and Title 18, United States Code, Section 981(a)(1)(C).

SUBSTITUTE PROPERTY

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

(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 substantially diminished in value; or

(e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 18, United States Code, Section 1963(m), the procedures of Title 21, United States Code, Section 853(p), and Rule 32.2 Fed. R. Crim. P., to seek forfeiture of any other property of said defendants up to the value of the forfeitable property described above.

_____
Daniel S. Wierzbicki
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this _____ day of May, 2011

_____
HON. ALAN KAY
UNITED STATES MAGISTRATE JUDGE