CR 12 (Rev. 5/03)

WARRANT FOR ARREST

United States District Court	DISTRICT: SOUTHERN DISTRICT OF NEW YORK
UNITED STATES OF AMERICA V.	DOCKET NO.: 12 MAG 1566 — MAGISTRATE'S CASE NO.
NIKHIL KOLBEKAR, a/k/a "N1kh1l," a/k/a "A!!3natedBuddh@," a/k/a "Rapid," a/k/a "Gh0sT," a/k/a "HellsAngel,"	NAME AND ADDRESS OF INDIVIDUAL TO BE ARRESTED: NIKHIL KOLBEKAR, a/k/a "N1kh1l," a/k/a "A!!3natedBuddh@," a/k/a "Rapid," a/k/a "Gh0sT," a/k/a "HellsAngel,"
WARRANT ISSUED ON THE BASIS OF: ☐ Order of Court ☐ Indictment ☐ Information [X] Complaint	DISTRICT OF ARREST
TO: UNITED STATES MARSHAL OR ANY OTHER AUTHORIZED OFFICER	CITY

YOU ARE HEREBY COMMANDED to arrest the above-named person and bring that person before the United States District Court to answer to the charge(s) listed below.

DESCRIPTION OF CHARGES

Conspiracy to commit computer hacking
Computer hacking

IN VIOLATION OF	UNITED STATES CODE TITLES: 18	SECTIONS: 1030(b), 1030(a)(5)(A), 1030(a)(6)(A), 1030(c)(2)(A), 1030(c)(4)(B)(i), 1030(c)(4)(A)(V1), and 2.
BAIL	OTHER CONDITIONS OF RELEASE	
ORDERED BY	SIGNATURE (FEDERAL JUDGE/U.S. MAGISTRATE): Frank Maas	DATE ORDERED: JUN 12 2012
CLERK OF COURT	(BY) DEPUTY CLERK	DATE ISSUED

RETURN

This warrant was received and executed with the arrest of the above-named person.

DATE RECEIVED	NAME AND TITLE OF ARRESTING OFFICER	SIGNATURE OF ARRESTING OFFICER
DATE EXECUTED		

Note: The arresting officer is directed to serve the attached copy of the charge on the defendant at the time this warrant is executed.

12 MAG 1566

Approved: _____
James J. Pastore, Jr.
Assistant United States Attorney

Before: HONORABLE KEVIN NATHANIEL FOX
United States Magistrate Judge
Southern District of New York

UNITED STATES OF AMERICA :	
	SEALED COMPLAINT
- v. - :	
	Violations of
NIKHIL KOLBEKAR, :	18 U.S.C. §§ 1030 and 2
a/k/a "N1kh1l,"	
a/k/a "A1!3natedBuddh@," :	COUNTY OF OFFENSE:
a/k/a "Rapid,"	New York
a/k/a "Gh0sT," :	
a/k/a "HellsAngel,"	
:	
Defendant.	

SOUTHERN DISTRICT OF NEW YORK, ss.:

PATRICK HOFFMAN, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE
(Conspiracy to Commit Computer Hacking)

1. From at least in or about June 2010, up to and including in or about June 2012, in the Southern District of New York and elsewhere, NIKHIL KOLBEKAR, a/k/a "N1kh1l," a/k/a "A1!3natedBuddh@," a/k/a "Rapid," a/k/a "Gh0sT," a/k/a "HellsAngel," the defendant, and others known and unknown, willfully and knowingly, combined, conspired, confederated, and agreed together and with each other to engage in computer hacking, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

2. It was a part and object of the conspiracy that NIKHIL KOLBEKAR, a/k/a "N1kh1l," a/k/a "A1!3natedBuddh@," a/k/a "Rapid," a/k/a "Gh0sT," a/k/a "HellsAngel," the defendant, and others known and unknown, would and did knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, would and did intentionally cause damage without

authorization to a protected computer, and would and did cause damage affecting 10 and more protected computers during a one-year period, to wit, KOLBEKAR sold and distributed log-in credentials that allowed computers to be accessed and remotely controlled without the computer owners' authorization.

OVERT ACTS

3. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about April 23, 2011, NIKHIL KOLBEKAR, a/k/a "N1kh1l," a/k/a "Al!3natedBuddh@," a/k/a "Rapid," a/k/a "Gh0sT," a/k/a "HellsAngel," the defendant, sent an electronic message through a computer located in New York, New York to a co-conspirator not identified herein ("CC-1").

b. On or about April 27, 2011, KOLBEKAR sent an electronic message through a computer located in New York, New York to a co-conspirator not identified herein ("CC-2").

c. On or about August 2, 2011, a co-conspirator not identified herein ("CC-3") sent an electronic message through a computer located in New York, New York to KOLBEKAR.

(Title 18, United States Code, Sections 1030(b), 1030(a)(5)(A), 1030(c)(4)(B)(i), and 1030(c)(4)(A)(VI).)

COUNT TWO
(Computer Hacking)

4. From at least in or about June 2010, up to and including in or about June 2012, in the Southern District of New York and elsewhere, NIKHIL KOLBEKAR, a/k/a "N1kh1l," a/k/a "Al!3natedBuddh@," a/k/a "Rapid," a/k/a "Gh0sT," a/k/a "HellsAngel," the defendant, 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, and thereby caused damage affecting 10 and more protected computers during a one-year period, to wit, KOLBEKAR distributed log-in credentials that allowed computers to be accessed and remotely controlled without the computer owners' authorization.

(Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i), 1030(c)(4)(A)(VI), and 2.)

COUNT THREE
(Trafficking in Passwords)

5. In or about June 2010, in the Southern District of New York and elsewhere, NIKHIL KOLBEKAR, a/k/a "N1kh1l," a/k/a "Al!3natedBuddh@," a/k/a "Rapid," a/k/a "Gh0sT," a/k/a "HellsAngel," the defendant, knowingly and with intent to defraud trafficked in a password and similar information through which a computer may be accessed without authorization and such trafficking affected interstate and foreign commerce, to wit, KOLBEKAR distributed usernames and passwords for several types of online accounts, including accounts associated with video games, adult entertainment sites, email accounts, and Facebook accounts.

(Title 18, United States Code, Sections 1030(a)(6)(A), 1030(c)(2)(A), and 2.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

6. I have been a Special Agent with the FBI for approximately one year. For the past three months, I have been assigned to a computer intrusion squad in the FBI's New York Field Office. I have received training regarding computer fraud, white collar crimes, and computer hacking.

7. I have been personally involved in the investigation of this matter. This affidavit is based upon my investigation, my conversations with other law enforcement agents, and my examination of reports and records. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

BACKGROUND

8. Based on my training and experience, I have learned the following:

a. Carding: "Carding" refers to various criminal activities associated with stealing personal identification information and financial information belonging to other individuals – including the account information associated with credit cards, bank cards, debit cards, or other access devices –

and using that information to obtain money, goods, or services without the victims' authorization or consent. For example, a criminal might gain unauthorized access to (or "hack") a database maintained on a computer server and steal credit card numbers and other personal information stored in that database. The criminal can then use the stolen information to, among other things: (1) buy goods or services online; (2) manufacture counterfeit credit cards by encoding them with the stolen account information; (3) manufacture false identification documents (which can be used in turn to facilitate fraudulent purchases); or (4) sell the stolen information to others who intend to use it for criminal purposes. "Carding" refers to the foregoing criminal activity generally and encompasses a variety of federal offenses, including, but not limited to, identification document fraud, aggravated identity theft, access device fraud, computer hacking, wire fraud, and bank fraud.

b. Carding Forums: "Carding forums" are websites used by criminals engaged in carding ("carders") to facilitate their criminal activity. Carders use carding forums to, among other things: (1) exchange information related to carding, such as information concerning hacking methods or computer-security vulnerabilities that could be used to obtain personal identification information; and (2) buy and sell goods and services related to carding, for example, stolen credit card or debit card account numbers, hardware for creating counterfeit credit cards or debit cards, or goods bought with compromised credit card and debit card accounts. Carding forums often permit users to post public messages (postings that can be viewed by all users of the site), which are often grouped together in "threads." For example, a user who has stolen credit card numbers may start a "thread" by posting a public message offering to sell the numbers. Carding forums also often permit users to communicate one-to-one through so-called "private messages." Because carding forums are, in essence, marketplaces for illegal activities, access is typically restricted to avoid law enforcement surveillance. Typically, a prospective user seeking to join a carding forum can only do so if other, already established users "vouch" for the prospective user, or if the prospective user pays a sum of money to the operators of the carding forum. User accounts are typically identified by a username and access is restricted by password. Users of carding forums typically identify themselves on such forums using aliases or online nicknames ("nics").

9. Based on my participation in the investigation of this matter, I know the following:

a. In or about June 2010, the FBI established an undercover carding forum (the "UC Site"), enabling users to discuss various topics related to carding and to communicate offers to buy, sell, and exchange goods and services related to carding, among other things.

b. The FBI established the UC Site as an online meeting place where the FBI could locate cybercriminals, investigate and identify them, and disrupt their activities.[1] The UC Site was configured to allow the FBI to monitor and to record the discussion threads posted to the site, as well as private messages sent through the site between registered users. The UC Site also allowed the FBI to record the Internet protocol ("IP") addresses of users' computers when they accessed the site.[2]

c. Access to the UC Site was limited to registered members and required a username and password to gain entry. Various membership requirements were imposed from time to time to restrict site membership to individuals with established knowledge of carding techniques or interest in criminal activity. For example, at times new users were prevented from joining the site unless they were recommended by two existing users who had registered with the site, or unless they paid a registration fee.

d. New users registering with the UC Site were required to provide a valid e-mail address as part of the registration process. An e-mail message was sent to that email address containing registration instructions. In order to complete the registration process, the new user was required to open the e-mail, click on a link in it, and then enter an activation code specified in the e-mail message. The e-mail addresses entered by registered members of the site were collected by the FBI.

e. In the course of the undercover operation, the FBI contacted multiple affected institutions and/or individuals to advise them of discovered breaches in order to enable them to

---

[1] The registration process for the UC Site required users to agree to terms and conditions, including that their activities on the UC Site were subject to monitoring for any purpose.

[2] Every computer on the Internet is identified by a unique number called an Internet protocol ("IP") address, which is used to route information properly between computers.

take appropriate responsive and protective measures. Based on information obtained through the site, the FBI estimates that it helped financial institutions prevent many millions of dollars in losses from credit card fraud and other criminal activity, and has alerted specific individuals regarding breaches of their personal email or other accounts.

f. At all times relevant to this Complaint, the server for the UC Site, through which all public and private messages on the UC Site were transmitted, was located in New York, New York.

THE INVESTIGATION

10. As discussed in detail below, the investigation has revealed that NIKHIL KOLBEKAR, a/k/a "N1kh1l," a/k/a "Al!3natedBuddh@," a/k/a "Rapid," a/k/a "Gh0sT," a/k/a "HellsAngel," the defendant, sold log-in credentials that allowed hackers to take over other computers through a program known as the Remote Desktop Protocol ("RDP"). KOLBEKAR also distributed usernames and passwords for several types of online accounts, including accounts associated with video games, adult entertainment sites, email accounts, and Facebook accounts. Finally, KOLBEKAR provided access to a software program that would automatically search for computer systems that were vulnerable to a type of cyberattack known as a "SQL injection." A "SQL injection" is a type of computer code that allows hackers to, among other things, gain unauthorized access to databases associated with websites.

11. From reviewing a copy of an online chat that occurred over MSN - a popular instant messaging service - I have learned, in substance and among other things:

a. On or about April 3, 2011, an individual using an MSN account named gh0st@fbi.al ("Gh0st") contacted an administrator of the UC Site, who in fact was a Special Agent of the FBI ("Agent-1") acting in an undercover capacity. As discussed in more detail below, "Gh0st" was subsequently identified as NIKHIL KOLBEKAR, a/k/a "N1kh1l," a/k/a "Al!3natedBuddh@," a/k/a "Rapid," a/k/a "Gh0sT," a/k/a "HellsAngel," the defendant.

b. During the chat, "Gh0st" wrote, "im now selling rdp. wondering if I cld get vereified."[3] ("Gh0st" previously had contacted Agent-1 in or about November 18, 2010 using the same MSN account, and wrote, among other things, "Its Gh0st from [the UC Site.]"). Based on my training and experience, and my familiarity with this investigation, I believe that "RDP" is a reference to "remote desktop protocol," which, as noted above, is a program that allows for remote control of a computer. More specifically, a user can remotely access a computer using RDP by providing the IP address of the computer, as well as a username and password to log into the computer through RDP.

c. From my training and experience, I know that RDP has several legitimate uses: for instance, it can be used to enable employees of a company to remotely log into their work computers. Hackers, however, can use RDP to gain control of a computer, and then use that compromised computer to conduct hacking or other criminal activity. In this way, the criminal activity appears to emanate from the compromised computer rather than the hacker's own computer, thus obscuring the hacker's identity and true location.

d. I also believe that "Gh0st's" reference to getting "verified" was a reference to the process that "vendors" on the UC Site had to follow in order to be approved to sell goods and services. Specifically, vendors on the UC Site had to submit their goods or services to administrators of the UC Site for review, in order to prove that the goods and/or services worked as advertised.

e. During the April 3, 2011 MSN chat, "Gh0st" provided the IP addresses, usernames and passwords for five computers that could be controlled using RDP. Agent-1 verified that at least three of the credentials could in fact be used to access computers using RDP. Agent-1 wrote to "Gh0st" that the connection speed to the computers using RDP was "kinda slow." "Gh0st" responded, "yea bro. . the country and speed specific ones will be charged at a higherr rate." Based on my training and experience, and my familiarity with this investigation, I believe that "Gh0st" was explaining that he would charge higher rates for faster connection speeds, and for computers that were located in specific countries. "Gh0st" ultimately began selling RDP log-in credentials (i.e., IP addresses, usernames and passwords) through the UC Site in or about April 2011.

---

[3] Quotations from emails and online postings are reproduced substantially as they appear in the original text; that is, errors in spelling and punctuation have not been corrected.

12. On or about April 3, 2011, NIKHIL KOLBEKAR, a/k/a "N1kh1l," a/k/a "A1!3natedBuddh@," a/k/a "Rapid," a/k/a "Gh0sT," a/k/a "HellsAngel," the defendant, utilizing the nickname "Gh0st," posted on the UC Site a thread titled "Worldwide RdP [Dont let the feds trace you]." The body of the thread read:

> Worldwide Rpd's availabe for sale
>
> Countries Available : Spain, Sweden, Italy, France, Germany, Brazil, South Africa, Czech Republic, India, Turkey.
>
> Need an RDP from a country not on the list / Faster Server / Config . DO NOT worry.
>
> Submit a request and it will be available for a premium price.
>
> Payment Method :liberty Reserve
>
> Pre-checked Prior to sale.
>
> Minimum Purchase : 50 rdp's
>
> No Refunds / No Guarantee

Based on my training and experience, and my familiarity with this investigation, I believe that, in the foregoing post, the defendant was advertising RDPs for sale in several countries. When the defendant wrote that the payment method was "liberty reserve," I believe that he was referring to a type of online currency known as Liberty Reserve. Finally, when the defendant wrote that the "minimum purchase" was "50 rdp's," I believe he meant that he sold only at least 50 RDPs at a time. In other words, the defendant had unauthorized access to at least 50 computers using RDP.

13. Private messages from the UC Site confirm that NIKHIL KOLBEKAR, a/k/a "N1kh1l," a/k/a "A1!3natedBuddh@," a/k/a "Rapid," a/k/a "Gh0sT," a/k/a "HellsAngel," the defendant, sold, and attempted to sell, RDP log-in credentials. For example:

a. On or about April 23, 2011, KOLBEKAR sent a private message through the UC Site to a co-conspirator not identified herein ("CC-1") in which KOLBEKAR sold RDP log-in credentials for one computer to CC-1 in exchange for $3.

b. On or about April 27, 2011, KOLBEKAR sent a private message through the UC Site to a co-conspirator not

identified herein ("CC-2"), in which KOLBEKAR offered to sell RDP log-in credentials for computers located in Africa and Brazil.

c. On or about August 2, 2011, a co-conspirator not identified herein ("CC-3") sent a private message through the UC Site to KOLBEKAR in which CC-3 sought to buy RDP log-in credentials for two computers.

14. NIKHIL KOLBEKAR, a/k/a "N1kh1l," a/k/a "Al!3natedBuddh@," a/k/a "Rapid," a/k/a "Gh0sT," a/k/a "HellsAngel," the defendant, also took steps to enhance his reputation on the UC Site by providing usernames, passwords and hacking tools free-of-charge to other users of the UC Site. Based on my training and experience, and my familiarity with this investigation, I have learned that hackers often attempt to establish their credibility on carding forums, and to encourage others to use their paid services, by providing, free-of-charge, valuable information including compromised credit account numbers, usernames and passwords for online accounts, and other hacking tools. Typically, hackers will publicly post this information in a thread, sometimes referred to as a "share." This free information serves, in essence, as an advertisement for the hacker's paid services by demonstrating that the hacker has the capability to hack into computer systems and obtain victims' personal information.

15. On or about June 15, 2010, NIKHIL KOLBEKAR, a/k/a "N1kh1l," a/k/a "Al!3natedBuddh@," a/k/a "Rapid," a/k/a "Gh0sT," a/k/a "HellsAngel," the defendant, utilizing the nickname "N1kh1l," posted on the UC Site a thread titled "F!rsT Acc0unT DumP" (the "June 15 Post"). The body of the thread read, in part, "Random Account Dump" and included, among other things, usernames and passwords for accounts at Facebook, gmail, hotmail, Yahoo, AOL, MySpace, a gaming website for Modern Warfare 2, World of Warcraft, and many other online services. In total, there were more than 75 usernames and passwords in the June 15 Post. I believe that KOLBEKAR was distributing the usernames and passwords for free in order to enhance his reputation on the UC Site.

16. Similarly, on or about November 13, 2010, NIKHIL KOLBEKAR, a/k/a "N1kh1l," a/k/a "Al!3natedBuddh@," a/k/a "Rapid," a/k/a "Gh0sT," a/k/a "HellsAngel," the defendant, utilizing the nickname "Gh0st," posted on the UC Site a thread titled, "Havij 1.13 Pro" (the "November 13 Post"). From my training and experience, I have learned, in substance and among other things, that Havij is a hacking tool that finds "SQL injection"

vulnerabilities in websites. That understanding is confirmed by the body of the November 13 Post, which reads, in part:

> Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a webpage. . . . By using this software user can perform back-end database fingerprint, retrieve DBMS users and password hashes, dump tables, fetching data from the database, running SQL statements and even accessing the underlying file system and executing commands on the operating system. . . .

17. The November 13 Post included a link to a purportedly "cracked" version of Havij - that is, a version that users could download free-of-charge instead of being required to pay for the hacking tool. In other words, the defendant did not himself create Havij, but instead provided users of the UC Site with a link at which they could download the hacking tool without paying for it.

Identification of the Defendant

18. From reviewing registration records for the UC Site, I have learned, in substance and among other things, that, on or about June 12, 2010, the username "N1kh1l" was registered with the UC Site, and getaafix@gmail.com was provided as a contact email address for the account. Records from the UC Site revealed that "N1kh1l" changed his username several times between June 2010 and May 2012, including on or about June 15, 2010 when he adopted the username "Al!3natedBuddh@"; on or about August 7, 2010, when he adopted the username "Rapid"; on or about October 8, 2010, when he adopted the username "Gh0sT"; and on or about August 16, 2011, when he adopted the username "HellsAngel."

19. During the investigation, the Government obtained a search warrant for the email account getaafix@gmail.com. From reviewing emails obtained pursuant to that search warrant, and from speaking with another Special Agent of the FBI ("Agent-2") who also reviewed emails contained in the getaafix@gmail.com account, I have learned, in substance and among other things:

a. An email dated March 8, 2011 was sent from getaafix@gmail.com to "dogtags@oliveplanet.in," a company that manufactures, among other things, dog tags (the "Dog Tag Email"). The user of the getaafix@gmail.com account wrote, in part, "Hello i just purchased dog tags form you guys on ebay."

The email then provided details for the order, including the following:

> Tag 2
> LINE 1: NIKHIL
> LINE 2: KOLBEKAR
> LINE 3: 27/8 TBS
> LINE 4: ANDHERI
> LINE 5: MUMBAI - INDIA

The Dog Tag Email also contained the following information in a section labeled "shipping address":

> Mr Nikhil Kolbekar
> # 27/8, Sadashiv sadan,
> Tarun bharat soc ,
> . . .
> Chakala andheri East,
> Mumbai 400099

It thus appears to me that NIKHIL KOLBEKAR, a/k/a "N1kh1l," a/k/a "A1!3natedBuddh@," a/k/a "Rapid," a/k/a "Gh0sT," a/k/a "HellsAngel," the defendant, ordered dog tags that contained his true name and address. More specifically, the Dog Tag Email indicated that "LINE 3" of the dog tags KOLBEKAR ordered read "27/8 TBS." That information corresponds to the address that KOLBEKAR provided in the "shipping address" section of his email: "#27/8" at the "Tarun bharat soc." Based on searches using publicly available databases, I believe "Tarun bharat soc" is short for the "Tarun Bharat Society," which is located in Chakala Andheri East, a suburb of Mumbai, India. That interpretation is further confirmed by the portion of the Dog Tag Email which indicated that lines 4 and 5 of the dog tags read "Andheri, Mumbai - India," as well as the "shipping address" information contained in the Dog Tag Email, which listed KOLBEKAR's address as located in "Chakala andheri East, Mumbai." That the email contains information about an order for dog tags, which are typically worn as a form of identification, further supports the conclusion that NIKHIL KOLBEKAR is the defendant's true name.

b. Several other emails in the getaafix@gmail.com also referred to "Nikhil Kolbekar," and listed as his address the same address that appeared in the Dog Tag Email. For instance, an email dated February 2, 2011, was sent from eBay, an online auction company, to getaafix@gmail.com. The email contained a receipt for a purchase made by "Nikhil Kolbekar," and read, in part:

The seller will deliver the item to the following address:
nikhil kolbekar
27/3 sadashiv Sadan Tarun bharat soc
Chakala Andheri east
Mumbai, MH 400099 IN

c. Another email, which was dated March 28, 2011, was sent from Freecharge, an Indian company that allows mobile phone users to purchase additional minutes for their mobile phones, to getaafix@gmail.com. The email read, in part:

Dear nikhil kolbekar,

Your account details has been changed on freecharge.
Your new details are given below :
Name: nikhil kolbekar
Address: 27/ 8 sadashiv sadan Tarun bharat society
CHakala andheri east
City: Mumbai

d. Another email, which was dated December 6, 2011, was sent from Dell, a computer company, to getaafix@gmail.com. The email contained purchase details for a Dell computer and indicated that the computer was going to be shipped to "Nikhil Kolbekar" at "Plot No. 27 3rd Floor Sadashiv Sadan, Tarun Bharat Society Chakala," in "SAHAR, 400099."

20. Posts to the UC Site also confirm that the defendant's true identity is NIKHIL KOLBEKAR. For example, on or about June 19, 2010, "Al!3natedBuddh@" replied to a thread on the UC Site regarding the sale of stolen iPhones. "Al!3natedBuddh@" signed the post "Nikhil."

WHEREFORE, I respectfully request that an arrest warrant be issued for NIKHIL KOLBEKAR, a/k/a "N1kh1l," a/k/a "Al!3natedBuddh@," a/k/a "Rapid," a/k/a "Gh0sT," a/k/a "HellsAngel," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.

PATRICK HOFFMAN
Special Agent
Federal Bureau of Investigation

Sworn to before me this
12th day of June 2012

HON. KEVIN NATHANIEL FOX
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK