CR 12 (Rev. 5/03)

WARRANT FOR ARREST

United States District Court	DISTRICT: SOUTHERN DISTRICT OF NEW YORK
UNITED STATES OF AMERICA v. JUSTIN MILLS, a/k/a "xTGxKAKAROT"	DOCKET NO.: 12 MAG 1653 — MAGISTRATE'S CASE NO.:
WARRANT ISSUED ON THE BASIS OF: ☐ Order of Court ☐ Indictment ☐ Information ☒ Complaint	NAME AND ADDRESS OF INDIVIDUAL TO BE ARRESTED: JUSTIN MILLS, a/k/a "xTGxKAKAROT", 94 Red Maple Road, Smyrna, DE 19977
	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

Trafficking in Passwords and Similar Information,
Access Device Fraud

IN VIOLATION OF	UNITED STATES CODE TITLE: 18	SECTION: 1030(a)(6) & 1029(a)(2)
BAIL	OTHER CONDITIONS OF RELEASE	
ORDERED BY: ANDREW J. PECK UNITED STATES MAGISTRATE JUDGE SOUTHERN DISTRICT OF NEW YORK	SIGNATURE (FEDERAL JUDGE/U.S. MAGISTRATE)	DATE ORDERED: JUN 20 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.

Approved: _____
SERRIN TURNER
Assistant United States Attorney

12 MAG 1653

Before: HONORABLE ANDREW J. PECK
United States Magistrate Judge
Southern District of New York

UNITED STATES OF AMERICA	:	SEALED COMPLAINT
- v. -	:	Violations of 18 U.S.C. §§ 1030(a)(6) & 1029(a)(2)
JUSTIN MILLS, a/k/a "xTGxKAKAROT,"	:	
Defendant.	:	COUNTY OF OFFENSE: New York

SOUTHERN DISTRICT OF NEW YORK, ss.:

Patrick D. 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
(Trafficking in Passwords and Similar Information)

1. From in or about November 2010, up to and including in or about March 2012, in the Southern District of New York and elsewhere, JUSTIN MILLS, a/k/a "xTGxKAKAROT," the defendant, knowingly and with intent to defraud, trafficked in passwords and similar information through which a computer may be accessed without authorization, in an offense affecting interstate and foreign commerce, to wit, MILLS sold stolen usernames and passwords that could be used to access accounts without authorization at various financial, shopping, and social networking websites.

(Title 18, United States Code, Section 1030(a)(6).)

COUNT TWO
(Access Device Fraud)

2. From in or about November 2010, up to and including in or about March 2012, in the Southern District of New York and elsewhere, JUSTIN MILLS, a/k/a "xTGxKAKAROT," the defendant, knowingly and with intent to defraud, trafficked in and used one and more unauthorized access devices during a one-year period affecting interstate and foreign commerce, and by such conduct obtained things of value aggregating $1,000 and more during that period, to wit, MILLS sold stolen credit card numbers, usernames, and passwords to others, and he used stolen credit card numbers, usernames, and passwords to purchase gift cards and goods that he sold to others, and by such conduct he obtained things of value aggregating $1,000 and more during a one-year period.

(Title 18, United States Code, Section 1029(a)(2) and 2.)

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

3. 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.

4. I have been a Special Agent with the FBI for over one year. I am currently been assigned to the computer intrusion squad in the FBI's New York Field Office. I have received training regarding computer technology, computer fraud, and white collar crimes.

Background on the UC Site

5. 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), sometimes referred to as "threads." For example, a user who has stolen credit card numbers may post a public "thread" 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").

6. 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.

Summary of the Investigation of "xTGxKAKAROT"

7. On or about October 4, 2010, an individual later identified as JUSTIN MILLS, the defendant, registered on the UC Site with the username "xTGxKAKAROT." "xTGxKAKAROT" provided his e-mail address as "justinmills5021@hotmail.com" for the purpose of receiving registration instructions.

8. As set forth below, the investigation has shown that JUSTIN MILLS, a/k/a "xTGxKAKAROT," the defendant, trafficked in stolen usernames and passwords that could be used to access without authorization various types of online accounts, and that MILLS also trafficked in stolen credit card data. Further, MILLS used these access devices to effect fraudulent purchases of gift cards and goods on the Internet, which he sold to others.

Trafficking in Login Information by "xTGxKAKAROT"

9. Based on my participation in the investigation of this matter, I know that the UC Site, consistent with practices on other carding forums, allowed users wishing to sell goods or services on the UC Site to become "authenticated sellers," by submitting their goods or services for review by a site administrator. (In actuality, the site administrator would be either an undercover agent or a cooperating witness in the investigation.) If the site administrator determined that the goods or services offered by the user were as advertised, the user could represent himself as an "authenticated seller" of the goods or services on the UC Site. Among other things, this process enabled the FBI to obtain evidence of the user's criminal activity and to analyze carding hardware, software, and methods submitted for authentication.

10. On or about October 30, 2011, "xTGxKAKAROT" sent a private message to a cooperating witness acting as a site

administrator of the UC Site ("CW-1").[3] In the message, "xTGxKAKAROT" stated that he wanted to become an "authenticated seller" of "[a]ccounts/logs" on the UC Site.[4] Based on my training and experience, I know that the term "logs" is commonly used by carders to refer to stolen login information (that is, usernames and passwords) that can be used to access various types of online accounts.

11. On or about November 1, 2010, CW-1 replied to "xTGxKAKAROT's" private message, telling "xTGxKAKAROT" to contact CW-1 on MSN Messenger - a popular instant messaging, or "chat," service on the Internet - to discuss the issue further.

12. On or about November 3, 2010, "xTGxKAKAROT" chatted with CW-1 on MSN Messenger. From reviewing the chat, which was electronically preserved, I know the following:

a. The MSN Messenger username used by "xTGxKAKAROT" was "JustinMills5021@hotmail.com" - the same e-mail address used by "xTGxKAKAROT" to register with the UC Site.

b. During the chat, "xTGxKAKAROT" stated that he had "170k logs" for sale, meaning, based on my training and experience, that he had 170,000 username/password combinations for sale.

c. CW-1 asked "xTGxKAKAROT" whether his logs included usernames and passwords for financial websites. "xTGxKAKAROT" replied affirmatively, stating, "ive got tons of chase and bank of America etc."

d. In commenting on his sales of logs to date, "xTGxKAKAROT" stated that "[m]ost of the time i sell bulk for cheap" but "upon request i do some accounts for $1." Based on

---

[3] Based on my involvement in this investigation, I know that CW-1 was arrested by law enforcement and agreed to cooperate with the Government in the hope of receiving a reduced sentence. CW-1 has pleaded guilty to various charges pursuant to a cooperation agreement with the Government and is awaiting sentencing. CW-1's involvement in chats and private messages relating to the UC Site was at the direction of, and monitored by, the FBI.

[4] Unless otherwise noted, all postings and private messages referred to herein were posted or sent on the UC Site and were retained as part of the operation of the UC Site. Quotations from such messages and any other electronic communications are reproduced substantially as they appear in the original text; errors in spelling and punctuation have not been corrected.

my training and experience, I understand "xTGxKAKAROT" to have meant that he usually sells bulk lists of "logs" covering a variety of websites, but that sometimes, for a buyer interested in accessing a particular website, he sells individual logs for that website for $1 each.

e. "xTGxKAKAROT" told CW-1 that he obtained his logs from "istealers." Based on my training and experience, I know that an "iStealer" is a form of malicious software, or "malware," that, if downloaded to a user's computer, can steal website login information stored in the user's Internet browser application. "xTGxKAKAROT" stated that he had "5 active istealers so i get more [logs] all the time." Based on my training and experience, I understand "xTGxKAKAROT" to have meant that he had five compromised computers infected with iStealer malware under his control, from which he was continuing to receive stolen login information.

f. CW-1 asked "xTGxKAKAROT" for a sample of his logs. In response, "xTGxKAKAROT" sent CW-1 a text file titled "iStealer_6.0_export.txt." The file, which I have reviewed, contains what appear to be approximately 700 username/password combinations for accounts at various websites, such as ebay.com and amazon.com.[5] The login information contained in the file is formatted in a manner that, based on my training and experience, indicates it was collected through iStealer software.

g. After telling "xTGxKAKAROT" that he had reviewed the username/passwords included in the text file, CW-1 informed "xTGxKAKAROT" that he was approving "xTGxKAKAROT" as an "authenticated seller" on the UC Site.

13. On or about November 4, 2010, xTGxKAKAROT" started a discussion thread titled, "170k Istealer Logs!!!!" His opening post stated:

> I [a]m selling 170,000 Logs[.] I will be selling these single and Bulk. I will be selling accounts upon Request so msn [MSN Messenger] and the pm [private message] system will be main source for Contact. I have Accounts to anything just let me kno what you need and i should have no problem in getting it.
>
> . . .

[5] The FBI has taken steps to alert the affected websites of the compromised account information.

Log Info: 2k+ Ebays 1k+ Amazon 10k+ Facebook (most have security questions tho) 1k+ Torrent Sites

Msn: Justinmills5021@hotmail.com

14. "xTGxKAKAROT" received numerous private messages in response to his November 4 post from UC Site users interested in purchasing his logs. "xTGxKAKAROT" typically responded to these users by instructing them to contact him via MSN Messenger to talk with him further about purchasing the logs.

15. In other communications on the UC Site, "xTGxKAKAROT" referred to sales of logs that he had consummated with other UC Site users:

a. On or about November 6, 2010, a UC Site user ("User-1") replied to "xTGxKAKAROT's" November 4 thread, asking if his logs included any accounts at "paypal" - an online payment processor. Later that day, "xTGxKAKAROT" replied to User-1, stating, "All paypals have been sold sorry."

b. On or about December 16, 2010, following a temporary outage of the UC Site, "xTGxKAKAROT" posted a message on his November 4 thread, stating: "Alright guys now that [the UC Site] is back up my sales are too[.] pm [private message] me if you need logs."

c. On or about December 19, 2010, "xTGxKAKAROT" sent a private message to CW-1 in which he told CW-1 that "im still selling my logs." "xTGxKAKAROT" and CW-1 continued their conversation by chatting on MSN Messenger later that day. From reviewing the chat, which was electronically preserved, I know that, during the chat, "xTGxKAKAROT" sent CW-1 a link to a text file containing what appear to be approximately 2,000 username/password combinations for accounts at various websites, including some of the same logs he had sent to CW-1 on November 4, 2010, as described above, but also including numerous additional logs that appear to have been freshly acquired.

Trafficking in and Use of Unauthorized Access Devices

16. On or about November 6, 2010, a UC Site user ("User-2") posted a discussion thread expressing interest in buying gift cards for various shopping websites from any UC Site users who could acquire them.

17. Later that same day, "xTGxKAKAROT" posted a response to User-2's discussion thread. In the posting, "xTGxKAKAROT" listed some of the websites identified by User-2 and stated, "I've got accounts to all those with purchese history so i might be able to get gc's to them." Based on my training and experience, I understand "xTGxKAKAROT" to have meant that he had login information for accounts at some of the websites User-2 was interested in, including accounts with purchase histories; "xTGxKAKAROT" believed that he could mine these purchase histories for credit card information that he could use in turn to purchase gift cards ("gc's") from the sites.

18. On or about February 3, 2011, "xTGxKAKAROT" started a discussion thread titled, "***Express GiftCards***." In his opening post, "xTGxKAKAROT" stated that he had 10 gift cards for sale from Express.com, a clothing store, each with a $200 face value. Five days later, on or about February 8, 2011, "xTGxKAKAROT" posted another message to the thread, announcing that he had sold the "last one."

19. On or about March 31, 2011, "xTGxKAKAROT" started a discussion thread titled, "New Sites!!!" In his opening post, "xTGxKAKAROT" stated that he had been "working lately to find tons of cardable sites" that other carders had not already discovered. "xTGxKAKAROT" stated that he was interested in either "selling the sites" - that is, selling information about the sites to other UC Site users interested in carding items on the sites - or "selling the items from the sites" - that is, selling items to other UC Site users that he himself had carded from the sites.

20. On or about April 27, 2011, a UC Site user ("User-3") started a discussion thread asking other UC Site users for advice on how to make "1000 a month or more" from carding. On or about May 2, 2011, "xTGxKAKAROT" replied to the thread, stating, "1k a month? If you need suggestions i can show you some ways to get that in a week." In a further posting by "xTGxKAKAROT" to this discussion thread on May 10, 2011, "xTGxKAKAROT" commented further about his carding activity, stating: "I can sell gc's [gift cards] or logs everyday and make some cash or wait til i find a cardable private store or a

exploit in security for a certain site . . . and make thousands then go on vacation lol [laughing out loud]."

21. On or about August 20, 2011, "xTGxKAKAROT" started a discussion thread titled, "Sony Vaio S Series." In the posting, "xTGxKAKAROT" stated that he had a Sony VAIO S-series laptop computer "brand new in factory sealing" available for sale. "xTGxKAKAROT" added, "Bidding Starts At: $700." After two days of bids by various users, "xTGxKAKAROT" posted to the thread on or about August 22, 2011, stating that a particular site user who had bid $900 had won the auction as the highest bidder.

22. On or about October 15, 2011, "xTGxKAKAROT" started a discussion thread titled, "HQ [high-quality] Cc's Visa,Mc,Amex,Disco." From reviewing the discussion thread, I know the following:

a. In his opening post, "xTGxKAKAROT" stated that he had credit card numbers for sale, including Visa and MasterCard numbers for $4.00 each and American Express and Discovery numbers for $4.50 each.

b. "xTGxKAKAROT" guaranteed that the card numbers were good, stating that he would "replace" any card numbers within 30 minutes after purchase if they turned out to be "dead or invalid." "xTGxKAKAROT" also represented that the balances on the cards for sale "should not be an issue."

c. On or about October 21, 2011, a UC Site user ("User-4") replied to the discussion thread with customer feedback, stating that he had obtained "Nice HQ [high-quality] cards" from "xTGxKAKAROT" and that his order "went through."

d. On December 16, 2011, another UC Site user ("User-5") replied to the discussion thread with customer feedback, stating of "xTGxKAKAROT": "He always has good cards. I never had any bad cards from him."

23. On or about February 7, 2012, "xTGxKAKAROT" started a discussion thread titled, "Pre Dropped Items 4 Sale." In the posting, "xTGxKAKAROT" advertised various items for sale, including, among other things, an iPad 2 for $450, a Microsoft Xbox videogame console for $150, and an iPod Touch for $150. "xTGxKAKAROT" stated that "[a]ll items are brand new and dropped." Based on my training and experience, by "dropped," I understand "xTGxKAKAROT" to have meant that the items had already been shipped to an address controlled by him by the original vendors. As a result, he could re-ship the items to

any secondary purchaser himself, as opposed to carding the items on behalf of the secondary purchaser and putting the secondary purchaser's shipping information on the order. Under this arrangement, the secondary purchaser would have no reason to fear that the original vendors of the items would be able to trace the items to the secondary purchaser's address.

24. During the course of the investigation, I obtained a search warrant for the "justinmills5021@hotmail.com" e-mail account that "xTGxKAKAROT" supplied in registering with the UC Site. In reviewing the contents of the account produced in response to the warrant, I discovered multiple e-mails containing lists of credit card accounts belonging to persons other than JUSTIN MILLS, a/k/a "xTGxKAKAROT," the defendant. For example, the search warrant return includes an outgoing email dated January 14, 2011, with the subject heading, "yo," containing a list of 32 credit card accounts, including the customer names, addresses, e-mail addresses, account numbers, expiration dates, and security codes associated with the accounts. I have confirmed with representatives of the relevant credit card companies that most of the credit card numbers listed in the e-mail correspond to genuine credit card accounts.[6]

Identification of "xTGxKAKAROT" and
Further Confirmation of His Carding Activity

25. I have reviewed documents received from a detective with the Delaware State Police ("Detective-1"), from which I have learned the following:

a. In or about December 2011, Detective-1 received information concerning a credit card fraud victim who reported several attempted unauthorized charges to his Visa credit card ("Victim-1"). Victim-1 reported that one of the attempted charges was for the purchase of an item that was to be shipped to a particular address in Smyrna, Delaware (the "Subject Address").

b. On or about December 16, 2011, Detective-1 visited the Subject Address, which was a residential address, and spoke with the residents there at the time. They identified themselves as the grandparents of JUSTIN MILLS, a/k/a "xTGxKAKAROT," the defendant. MILLS' grandparents told Detective-1 that MILLS resided at the address with them and

[6] The FBI has alerted the relevant credit card companies to the compromise of the accounts.

frequently received packages there, which he sometimes shipped back out a few days after receiving them. MILLS' grandparents showed Detective-1 to MILLS' room in the house and consented to Detective-1 searching it.

c. In searching MILLS' room, Detective-1 found numerous packages that appeared to have been recently delivered to the Subject Address. The packing slips and shipping labels had been removed from the majority of the packages. Among the items contained in the packages and seized by Detective-1 were the following:

- Six Rumba Time watches ($1,050 total face value)
- Five Superga MN shoes ($240 total face value)
- Four Turtle Beach Delta Programmable Wireless 7.1 Surround Sound Headsets ($1,200 total face value)
- Four Morphsuit outfits ($264 total face value)
- Two Dyson DC41 vacuum cleaners ($1,200 total face value)
- Two Apple iPad 2 devices ($1,424 total face value)
- One Amazon Kindle DX device ($540 face value)
- One Nokia E7 Cellphone ($500 face value)

26. In the days following Detective-1's search of MILLS' residence, various users of the UC Site began to post complaints that they had not received items owed to them by "xTGxKAKAROT." On or about December 29, 2011, "xTGxKAKAROT" posted a response to these complaints, stating that "an investigator" had gone "into my room" and taken "things that came and other things that were unopened laying in my room." "xTGxKAKAROT" added, "your little iPads [and] other things of mine are gone now."

27. Accordingly, I believe that the individual described above as "xTGxKAKAROT" is JUSTIN MILLS, a/k/a "xTGxKAKAROT," the defendant.

WHEREFORE, I respectfully request that an arrest warrant be issued for JUSTIN MILLS, a/k/a "xTGxKAKAROT," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.

PATRICK D. HOFFMAN
Special Agent
Federal Bureau of Investigation

Sworn to before me this
20th day of June 2012

UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK