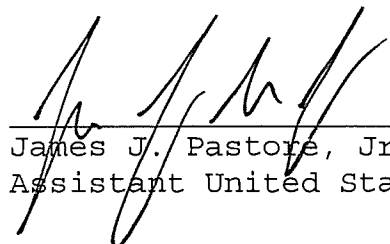


WARRANT FOR ARREST

United States District Court		DISTRICT SOUTHERN DISTRICT OF NEW YORK	
UNITED STATES OF AMERICA v. MICHAEL HOGUE, a/k/a "xVisceral"		DOCKET NO. 12 MAG 1632	MAGISTRATE'S CASE NO.
WARRANT ISSUED ON THE BASIS OF: <input type="checkbox"/> Order of Court <input type="checkbox"/> Indictment <input type="checkbox"/> Information <input checked="" type="checkbox"/> Complaint		NAME AND ADDRESS OF INDIVIDUAL TO BE ARRESTED MICHAEL HOGUE, a/k/a "xVisceral"	
TO: UNITED STATES MARSHAL OR ANY OTHER AUTHORIZED OFFICER		DISTRICT OF ARREST 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(c)(4)(B)(i) and (c)(4)(A)(i)(VI), and 2.	
ANDREW J. PECK, U.S. MAGISTRATE JUDGE ORDERED SOUTHERN DISTRICT OF NEW YORK		OTHER CONDITIONS OF RELEASE	
SIGNATURE (FEDERAL JUDGE/U.S. MAGISTRATE) <i>[Signature]</i>		DATE ORDERED JUN 18 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:


James J. Pastore, Jr.
Assistant United States Attorney

12 MAG 1632

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

- - - - - x
: UNITED STATES OF AMERICA : SEALED COMPLAINT
: :
- v. - : Violation of
: 18 U.S.C. §§ 1030 and 2
MICHAEL HOGUE, :
a/k/a "xVisceral," : COUNTY OF OFFENSE:
: New York
Defendant. :
: :
- - - - - x

SOUTHERN DISTRICT OF NEW YORK, ss.:

Jordan T. Loyd, 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 May 2012, in the Southern District of New York and elsewhere, MICHAEL HOGUE, a/k/a "xVisceral," the defendant, and others known and unknown, 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 an object of the conspiracy that MICHAEL HOGUE, a/k/a "xVisceral," the defendant, and others known and unknown, knowingly would and did 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, which would and did cause damage affecting 10 and more protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i) and (c)(4)(A)(i)(VI), to wit, HOGUE used malware to infect computers and sold that malware

to others, enabling them to infect and remotely control victims' computers.

(Title 18, United States Code, Section 1030(b).)

COUNT TWO
(Distribution of Malware)

3. From at least in or about June 2010, up to and including in or about May 2012, in the Southern District of New York and elsewhere, MICHAEL HOGUE, a/k/a "xVisceral," 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, HOGUE used malware to infect computers and sold that malware to others, enabling them to infect and remotely control victims' computers.

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

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

4. 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.

5. I have been a Special Agent with the FBI for approximately three years. For the past two years, I have 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

6. 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").

7. 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 buy, sell, and exchange goods and services related to carding, among other things.

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

c. 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 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 individuals regarding breaches of their email or other accounts.

d. 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 serious carding skills or interest in criminal activity. For example, at times new users were prevented from joining the site unless they were vouched for by two users who already had registered with the site or paid a registration fee.

e. 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

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.

complete the registration process, the new user had 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.

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

8. Based on my review of, among other things, posts to the UC Site, private messages, software provided by MICHAEL HOGUE, a/k/a "xVisceral," the defendant, and emails obtained pursuant to a search warrant, I have concluded that HOGUE sells malware that allows cybercriminals to take over and control, remotely, the operations of an infected computer. Such tools are sometimes known as remote access tools or "RATS."

9. The RAT distributed by MICHAEL HOGUE, a/k/a "xVisceral," the defendant, was a sophisticated piece of malware (the "RAT"). Based on the FBI's review of the RAT, I have learned, in substance and among other things:

a. One component of the RAT consisted of code that could be installed on a victim's computer, which enabled unauthorized access to that computer. Based on my review of the RAT, HOGUE provided the virus itself, but not the means of delivery. In other words, purchasers of the RAT had to determine on their own how to infect victims' computers with the malware. Based on my training and experience, I know that this could be accomplished in several ways, including by tricking victims into clicking on malicious links contained in emails sent to them, or by convincing victims to view a video or to visit a particular website where the malware resides, thereby causing it to install on their computers.

b. The RAT also featured a graphical user interface branded as "Blackshades Net," which allowed criminals to easily view and navigate all of the computers that they infected. Among other things, the user interface listed IP address information for each infected computer, the computer's name, the computer's operating system, the country in which the computer was located, and whether the computer contained a web camera.

10. In or about June 2010, MICHAEL HOGUE, a/k/a "xVisceral," the defendant, contacted an administrator of the UC Site who, unbeknownst to HOGUE, was in fact a Special Agent of

the FBI acting in an undercover capacity ("Agent-1"). Specifically, HOGUE wanted Agent-1 to review his RAT, so that HOGUE could become an approved "vendor" on the UC Site, which would allow him to advertise sale of the RAT on the UC Site.³

11. MICHAEL HOGUE, a/k/a "xVisceral," the defendant, communicated with Agent-1 through several means, including MSN, a popular instant messaging service. From reviewing logs of certain of the MSN chats, I have learned, in substance and among other things:

a. On or about June 30, 2010, HOGUE used the online nickname "admin@xvisceral.com" to communicate with Agent-1 via MSN.

b. During the June 30 chat, HOGUE provided a link to a location where the RAT could be downloaded, so that Agent-1, in his capacity as an administrator of the UC Site, could test the RAT.

c. Using the information HOGUE provided to Agent-1, I was able to review the RAT and confirmed that it was functional. HOGUE provided Agent-1 with the information necessary to view computers that HOGUE had infected (*i.e.*, to see how the RAT functioned). When I logged into the Blackshades Net service (that is, the interface that is a component of the RAT), I was able to see the names of 9 computers that had been infected with the malware component of the RAT. Those computers were located in Germany, the United States, Denmark, Poland, and Canada. (The FBI has taken steps to identify and locate these victims.) By clicking on the name of an infected computer, I was presented with a menu of options including the ability to initiate keylogging on the infected computer - that is, I was able to remotely turn on a service that would record every keystroke of the user of the infected computer. So, for instance, if the victim visited a banking website and entered his or her username and password, the keylogging program could

³ The UC Site allowed users wishing to regularly sell goods or services on the site to become "verified vendors" by submitting their goods or services for review by a site administrator (who, in actuality, would be either an undercover agent or a confidential source 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 a "verified vendor" on the UC Site. This process enabled the FBI to obtain evidence of the user's criminal activity and to investigate carding hardware, software, and methods.

record that information, which could then be used to access the victim's bank account.

d. Another online chat occurred between HOGUE and Agent-1 on or about July 2, 2010. From reviewing a copy of the chat, I have learned the following exchange took place during the chat:

Agent-1: do i have to manually keylog these machines or it does it auto?

HOGUE: it auto does, and you can download from all at once, or scan for keywords, or digits and if it detects a credit card is being entered it can send screenshots to FTP and you can scan for digits that are 16 in a row :P

Based on my training and experience, and my familiarity with this investigation, I believe that, in the foregoing exchange, HOGUE was explaining how the RAT was able to automatically capture keystrokes being entered by a victim who was using an infected computer, and, during that capture, the RAT could automatically detect when a victim was entering a credit card number. The RAT then took screenshots - meaning a copy of what was displayed on the victim's computer monitor - and sent those screenshots via FTP (which stands for "File Transfer Protocol") to the user of the RAT. In other words, the RAT was capable of automatically sending victims' credit card information to users of the RAT.

e. The following exchange also took place during the July 2, 2010 chat between HOGUE and Agent-1:

Agent-1: [H]ow many you currently have?

HOGUE: too much time spent with sales to ever attempt to get any :P maybe 50-100 through

Agent-1: ah ok. do other people have a lot?

HOGUE: yeah there are people with thousands.

Based on my training and experience, and my familiarity with this investigation, I believe that, in the foregoing exchange, HOGUE was telling Agent-1 that HOGUE had infected approximately 50 to 100 computers with the RAT, while other users of the RAT had infected and had been able to control "thousands" of computers.

12. From reviewing publicly available information as well as posts on the UC Site, I have learned, in substance and among other things, that MICHAEL HOGUE, a/k/a "xVisceral," the defendant, sold the RAT (typically for \$50 per copy) through several websites, including www.xvisceral.com, www.hackforums.net, www.blackshades.net, www.bshades.com, www.bshades.eu, and the UC Site. (On the UC Site, HOGUE advertised the malware under the username "xVisceral.") In addition, the RAT was available for download free-of-charge in so-called "cracked" versions (i.e., versions that had been hacked without HOGUE's permission) through, among other sites, www.opensc.ws, www.ubers.org, www.megapid.com, www.megaupload.com, www.4shared.com, www.filestube.com, www.133thackers.com, and www.freehacktools.com.

13. From reviewing a copy of the website located at www.xvisceral.com (the "xVisceral Website"), I have learned, in substance and among other things, that:

a. In or about December 2010, the homepage of the xVisceral Website featured a stylized logo that read "Blackshades Net" - the name of the interface for the RAT.

b. The xVisceral Website also contained several pages that extolled the benefits of the RAT, and included tutorials regarding how to use the RAT. For instance, the "Information" page of the xVisceral Website stated, among other things:

Deciding between a RAT, a host booter, or controlling a botnet has never been easier. With Blackshades NET, you get the best of all three - all in one with an easy to use, nice looking interface. You are able to choose between four crisp looking skins, with the default being a very nicely-fitting black theme. Even better, Blackshades NET does a lot of the work for you - it can automatically map your ports, seed your torrent for you, and spread through AIM, MSN, ICQ and USB devices. Don't know how to set up a RAT? Many people are here to help - and there are tutorials, too!⁴

Based on my training and experience, and my familiarity with this investigation, I know that a "botnet" is a

⁴ 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.

term used to refer to a group of infected computers. These infected computers are sometimes referred to as robots or "bots" for short because they can be directed to perform tasks without the true computer owners' permission.

c. The xVisceral Website also stated that the RAT could enable commands on infected computers including "Keylog Manager," "Webcam capture," and "File Infector."

d. The xVisceral Website also included information about upgraded or new versions of the RAT.

14. Based on records regarding the registration of the domain name www.xvisceral.com, I have learned that, in or about January 2010, it was registered to "Michael Hogue" at an address in Tucson, Arizona.

15. In addition, when "xVisceral" registered with the UC Site on or about June 13, 2010 he provided "blackshadesnet@hotmail.com" as his contact email address. The Government obtained a search warrant for that email account and, from reviewing the results of that search warrant, I have learned, in substance and among other things:

a. The email account contained more than two dozen emails from Amazon that were addressed to "Michael Hogue." In addition, many of those emails indicated that items had been shipped to "Michael Hogue" at an address in Tucson, Arizona ("Address-1").

b. The email account also contained emails from at least 10 individuals in which they were seeking assistance using the RAT. For instance, an email dated November 7, 2010 contained the subject "Buy rat." The body of the email read, in part, "i want to buy your rat..i'm using paypal..how to buy? please send the link.."

c. Another email read, in part:

Mike-

I have not used the BS in a while and noticed there is a ver 4.8 which I recently downloaded to see what i may of missed from my servers.

Based on my training and experience, and my familiarity with this investigation, I believe that "BS" is a reference to the Blackshades client. The fact that the email

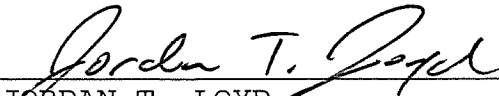
sender addressed the email to "Mike" further confirms that "xVisceral" is, in fact MICHAEL HOGUE, the defendant.

16. I also have reviewed subscriber records associated with an IP address that was used to log into blackshadesnet@hotmail.com (the "68.226 IP Address"). Those records indicated, among other things, that the 68.226 IP Address was subscribed to Address-1.

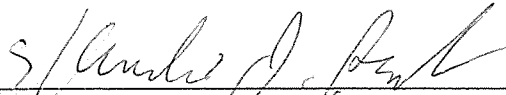
17. In addition to the xVisceral Website, I also reviewed a copy of a website that was located at www.bshades.com and have learned, in substance and among other things, that, at times relevant to this Complaint, MICHAEL HOGUE, a/k/a "xVisceral," the defendant, offered other services in addition to the RAT including: a password stealer, which was sometimes referred to as "Blackshades Stealer" or as "Blackshades Recovery" (because hackers "recover" other people's passwords); virtual private networks ("VPNs") that could be used to obfuscate the true location of a computer user; and a tool sometimes called the "Blackshades Network Stressor" that could be used to disable a website by overwhelming it with requests for information in what is known as a "distributed denial of service" ("DDoS") attack.

18. Since at least February 2012, MICHAEL HOGUE, a/k/a "xVisceral," the defendant, also sold Blackshades products and services through a website located at www.bshades.eu. That website also included a forum on which users posted comments and questions regarding Blackshades products. Among other things, users discussed how to avoid detection by anti-virus software on victim computers, and how to activate keylogging features in order to obtain passwords without authorization.

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


JORDAN T. LOYD
Special Agent
Federal Bureau of Investigation

Sworn to before me this
19th day of June 2012


HON. ANDREW J. PECK
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK