14 MAG 1064

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

Before: HONORABLE DEBRA FREEMAN
United States Magistrate Judge
Southern District of New York

UNITED STATES OF AMERICA	:	SEALED COMPLAINT
- v. -	:	Violation of 18 U.S.C. §§ 1030, 1029 and 2
KYLE FEDOREK, a/k/a "kbello,"	:	
Defendant.	:	COUNTY OF OFFENSE: New York

SOUTHERN DISTRICT OF NEW YORK, ss.:

NAVIN KALICHARAN, 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 September 2012, up to and including in or about March 2014, in the Southern District of New York and elsewhere, KYLE FEDOREK, a/k/a "kbello," the defendant, and others known and unknown, knowingly and willfully 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 KYLE FEDOREK, a/k/a "kbello," the defendant, and others known and unknown, knowingly and willfully 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, and 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, FEDOREK purchased malicious software,

or "malware," from an entity known as Blackshades and, relying on servers maintained by that organization, used the malware to infect victims' computers and steal information, including financial account information.

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 September 12, 2012, KYLE FEDOREK, a/k/a "kbello," purchased a copy of malicious software known as "Blackshades" over the Internet.

b. On or about June 30, 2010, a co-conspirator transmitted a copy of malicious software known as "Blackshades" to an FBI Special Agent located in New York, New York who was acting in an undercover capacity.

c. In or about 2013, an FBI Special Agent located in New York, New York purchased a copy of malicious software from a website maintained by Blackshades.

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

COUNT TWO
(Computer Hacking)

4. From at least in or about September 2012, up to and including in or about March 2014, in the Southern District of New York and elsewhere, KYLE FEDOREK, a/k/a "kbello," the defendant, 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 caused 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, FEDOREK used malicious software, or "malware," including Blackshades malware, to infect victims' computers and steal information, including financial account information.

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

COUNT THREE
(Access Device Fraud)

5. From at least in or about September 2012, up to and including in or about March 2014, in the Southern District of New York and elsewhere, KYLE FEDOREK, a/k/a "kbello," the defendant, knowingly and with intent to defraud possessed fifteen and more access devices which were counterfeit and unauthorized access devices, to wit, FEDOREK possessed at least thousands of access devices, including credit card numbers and financial account numbers, which were obtained through computer hacking.

(Title 18, United States Code, Sections 1029(a)(3) and 2.)

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

6. 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.

7. I have been a Special Agent with the FBI since approximately February 2009. Since approximately June 2013, I have been assigned to a computer intrusion squad in the FBI's New York Field Office. I have received training regarding computer technology, computer fraud, and white collar crimes. I have participated in the arrests of multiple individuals suspected of engaging in cybercrimes.

Overview

8. Since at least in or about 2010, an organization known as "Blackshades" has sold and distributed malicious software to thousands of cybercriminals throughout the world. Blackshades' flagship product was the Blackshades Remote Access Tool, or R.A.T. (the "RAT"), a sophisticated piece of malware that enabled cybercriminals to remotely and surreptitiously gain control over a victim's computer. After installing the RAT on a victim's computer, a user of the RAT had free rein to, among other things, access and view documents, photographs and other files on the victim's computer, record all of the keystrokes entered on the victim's keyboard, steal the passwords to the victim's online

accounts, and even activate the victim's web camera to spy on the victim -- all of which could be done without the victim's knowledge.

9. The FBI's investigation has shown that the RAT was purchased by at least several thousand users in more than 100 countries and used to infect more than half a million computers worldwide. The FBI's investigation has included, among other things, the execution of physical search warrants and more than 100 e-mail search warrants, the seizure of more than 1,900 domain names used by purchasers of the RAT to control victims' computers, and the execution of a search warrant for a computer server controlled by Blackshades. Further, an undercover FBI agent in New York, New York obtained a copy of the RAT from one of the RAT's co-creators, who subsequently cooperated with the Government and provided extensive information about Blackshades ("CW-1").[1] The FBI's investigation has revealed that the Blackshades RAT was, in fact, used by Blackshades customers to, among other things, activate web cameras, steal files and account information, and log keystrokes.

10. KYLE FEDOREK, a/k/a "kbello," the defendant, was a customer of Blackshades who purchased the RAT in or about September 2012. From in or about September 2012 through in or about March 2014, when the FBI executed a search warrant at FEDOREK's home and seized his computer, FEDOREK used the RAT to steal financial and other account information from more than 400 victims. As detailed below, a search of FEDOREK's computer also revealed that FEDOREK was deploying a variety of other types of malicious software against his victims.

Background on the Blackshades RAT

11. The Blackshades RAT was advertised and discussed, among other places, on online forums for computer hackers. Copies of the RAT were available for sale, typically for $40 each, on the Blackshades website, which was located at, among

---

[1] CW-1 was arrested in June 2012 as part of a Government investigation known as "Operation Cardshop." In January 2013, CW-1 pled guilty to two counts of violating Title 18, United States Code, Section 1030 (computer hacking) pursuant to a cooperation agreement with the Government, in the hopes of obtaining a reduced sentence. CW-1 has proven to be reliable, and the information that CW-1 has provided has been corroborated by, among other things, emails and other information seized pursuant to search warrants, as well as logs of online chats seized from CW-1's computer.

other domains, www.blackshades.ru and www.bshades.eu (the "Blackshades Website"). The RAT was typically advertised as a product that conveniently combined the features of several different types of hacking tools. For instance, one online advertisement read:

> Deciding between a RAT, a host booter, or controlling a botnet has never been easier.[2] With Blackshades . . . you get the best of all three - all in one with an easy to use, nice looking interface.
>
> Even better, Blackshades . . . does a lot of work for you - it can automatically map your ports, seed your torrent for you, and spread through AIM, MSN, ICQ and USB devices.

12. Based on my review of the Blackshades software, as well as information provided by CW-1, I know that, after purchasing a copy of the RAT, in order to use it, a user had to install the RAT on a victim's computer - i.e., "infect" a victim's computer. The infection of a victim's computer could be accomplished in several ways, including:

a. by tricking victims into clicking on malicious links contained in emails sent to them;

b. by convincing victims to click on links for videos or to visit websites that caused the malware to be installed; or

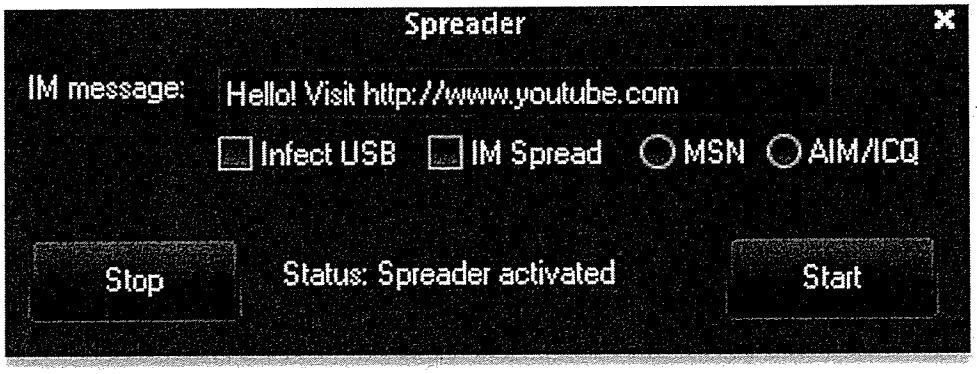
c. by hiring others to install the RAT on victims' computers, which at times Blackshades itself offered to do on behalf of its customers for an additional fee.

13. The RAT also contained tools known as "spreaders" that helped users of the RAT infect victim computers. The spreader tools generally worked by using computers that had already been infected to help spread the RAT further to other computers. For instance, as depicted below, in order to lure people to click on malicious links that would install the RAT on their computers, the RAT allowed users to send those malicious links to others via

---

[2] A "host booter" is a tool that can be used to launch a denial of service (or "DoS") attack, typically in the context of online video games. It disconnects or "boots" a person from a "host" (e.g., an online video game platform) and is typically done to cheat at the video game. A "botnet" typically refers to a network of infected computers or "bots."

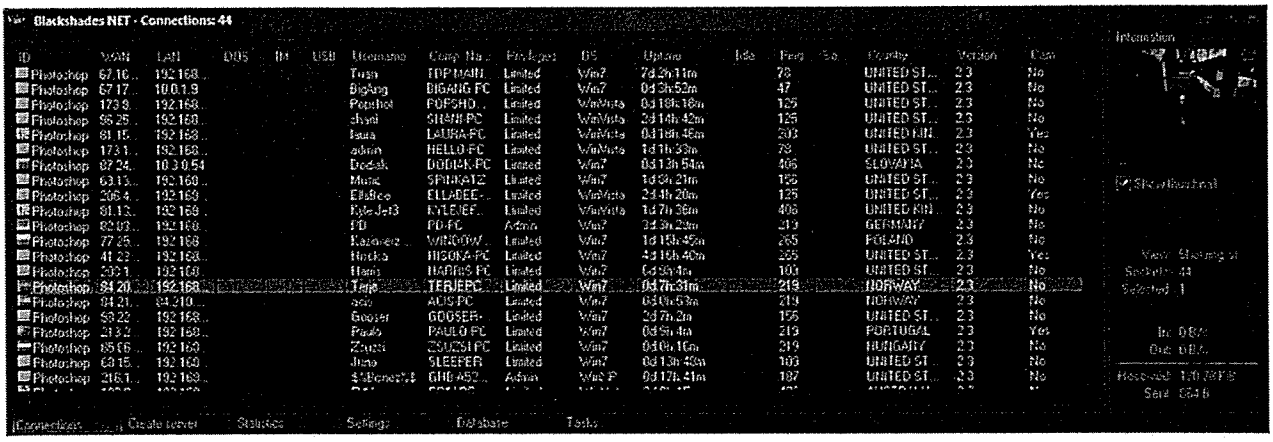
a victim's social media service, making it appear as if the message had come from the victim's compromised computer:



In this example, the user of the RAT has set the RAT to be spread through a malicious link that would be sent to others via the victim's instant messaging, or IM, services. In this case, the victim's social contacts would receive an IM message (purportedly from the victim), saying "Hello!" and inviting them to click on a link that appeared to lead to the YouTube website. In this way, the victim's friends might be fooled into clicking on the link purportedly sent by the victim, which would in fact install the RAT on that person's computer.

As can be seen above, the RAT's spreader feature also provided users an option to "Infect USB," which would infect any device plugged into a USB port on the victim's computer, such as a thumb drive. In this way, the malware could be spread between two computers through use of a thumb drive (e.g., a person's home and work computers).

14. The RAT also featured a graphical user interface, which allowed cybercriminals to easily view and navigate all of the victim computers that they had infected:



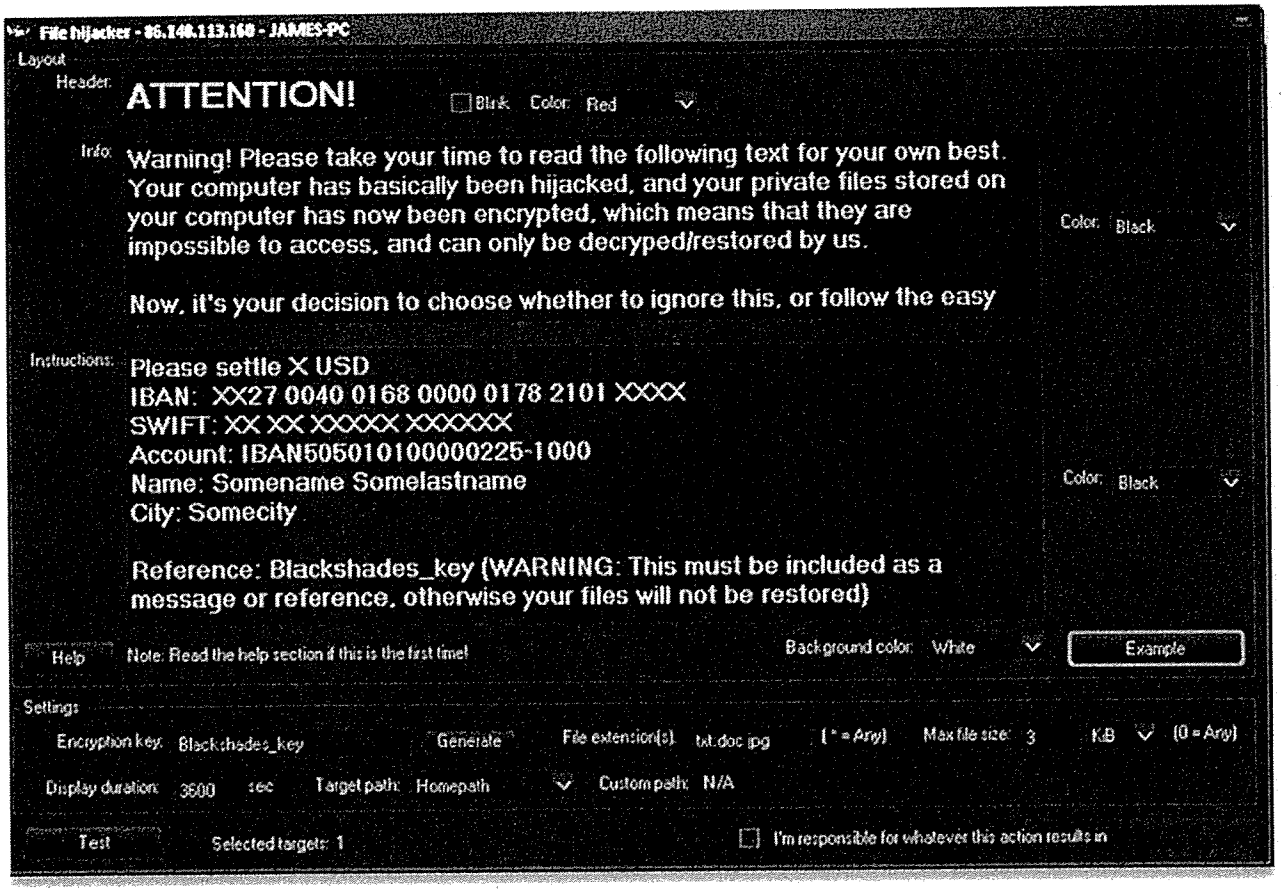
Among other things, the user interface[3] listed IP address information for each infected computer, the computer's name, the computer's operating system, the country in which the computer was located, and whether the computer had a web camera.

15. Once a computer was infected with the RAT, the user of the RAT could remotely activate the victim's web camera. By doing so, the RAT user could take photographs or obtain a live feed from the infected computer's web camera. In this way, the user could spy on anyone within view of the victim's webcam inside the victim's home or in any other private spaces where the victim's computer was used.

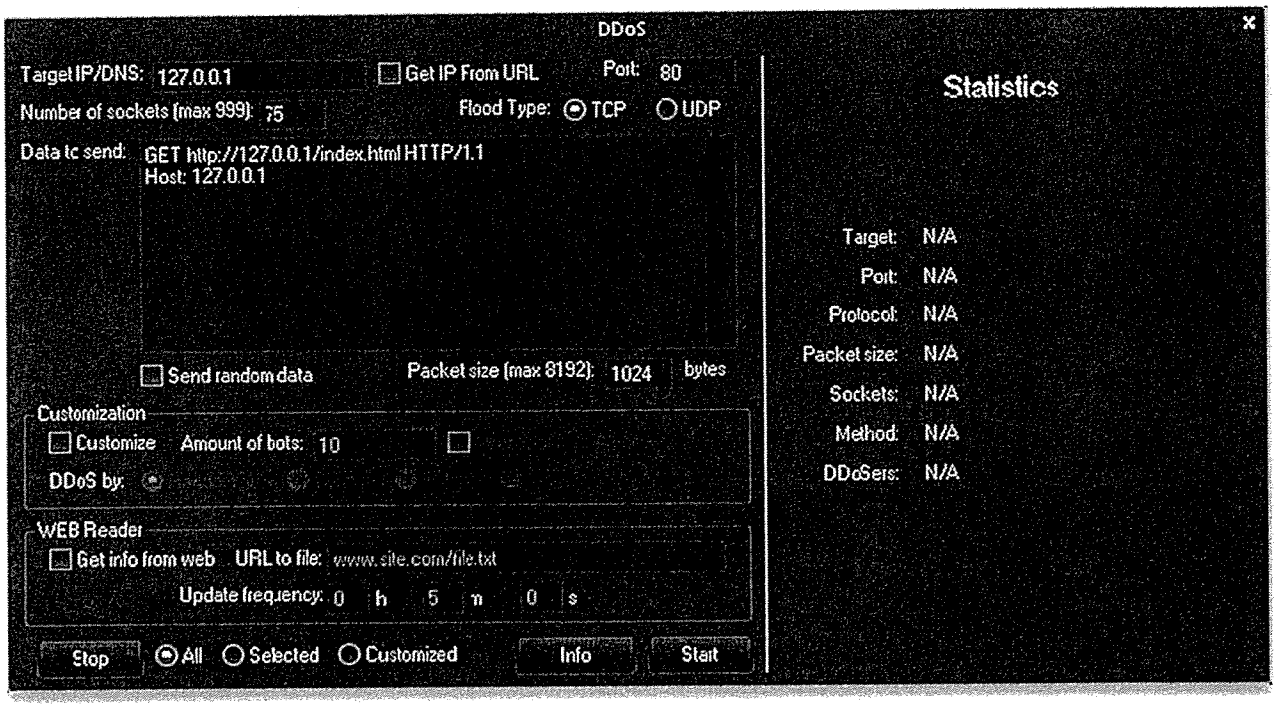
16. The RAT also contained a "keylogger" feature that allowed users to record each key that victims typed on their computer keyboards. To help users steal a victim's passwords and other log-in credentials, the RAT also had a "form grabber" feature. The "form grabber" automatically captured log-in information that victims entered into "forms" on their infected computers (e.g., log-in screens or order purchase screens for online accounts).

17. The RAT also provided its users with complete access to all of the files contained on a victim's computer. A RAT user could use such access to view or download photographs, documents, or other files on a victim's computer. Further, using a tool known as "file hijacker," the RAT enabled users to encrypt, or lock, a victim's files and demand a "ransom" to unlock them. This "ransomware" feature of the RAT included a pre-drafted ransom note that could be sent to victims:

[3] A copy of the interface is attached hereto as Exhibit A.



18. The RAT also allowed users to exploit victims' computers to launch other cyber attacks. Infected computers - which, as noted above, are sometimes referred to as "bots" - could be gathered into a network known as a "botnet." The botnet could then be used to launch Distributed Denial of Service ("DDoS") attacks against particular websites by repeatedly sending requests to the website in an effort to disable the website and deny service to legitimate customers. The RAT included a special DDoS tool that simplified the process of launching DDoS attacks using infected computers:



19. The RAT also included several features that were designed to harass or frighten victims. One feature, for example, allowed RAT users to "talk" to a victim through the victim's own infected computer by using the computer's "speech to text" feature. That is, a RAT user could type a message to the victim, and the victim's computer would read the message aloud. Another feature of the RAT caused an online chat window to appear on a victim's computer, through which the RAT user could type messages to the victim. The victim was unable to close, move, or otherwise remove the chat window.

Other Blackshades Products and Services

20. Based on the FBI's review of the Blackshades Website, as well as information provided by CW-1, I know that, in addition to the RAT, Blackshades has also sold Blackshades Crypter, a program designed to make the RAT undetectable by anti-virus software; Blackshades Stealth, a version of the RAT coded in certain programming languages that allowed the RAT to be controlled by Macs in addition to PCs; and Blackshades Fusion, malicious software designed to steal passwords, launch DDoS attacks, and capture webcam feeds, among other things.

21. Based on the FBI's review of a server controlled by Blackshades (the "Blackshades Server"), a copy of which was obtained by the FBI pursuant to a search warrant, I know that the Blackshades Server stored usernames and passwords of victims that had been stolen using Blackshades products. A Blackshades

customer could access and download to his or her computer the stolen usernames and passwords by logging into his or her Blackshades account.

22. From speaking with CW-1 and from reviewing the Blackshades Website, the FBI has also learned that from time to time Blackshades has provided a service known as a "Virtual Private Network" or "VPN." Based on my training and experience, I know that VPNs can be used to obscure the true IP address of a computer. Accordingly, cybercriminals often use VPNs to make it more difficult for law enforcement to identify their true IP addresses and physical locations.

The Blackshades Organization

23. Based on information provided by CW-1 and other witnesses, as well as records obtained pursuant to search warrants, I know that Blackshades operated as a business, which was owned and operated by Alex Yucel, a/k/a "marjinz." Among other things, Yucel hired and fired employees, paid employees' salaries, and updated the malicious software in response to customers' comments and requests. To facilitate the operations of the Blackshades organization, Yucel employed several paid administrators, including a director of marketing, website developer, customer service manager, and a team of customer service representatives. In addition to running the Blackshades organization, Yucel - along with CW-1 - created the RAT.

24. Based on the FBI's review of the Blackshades Website, information provided by CW-1, and records obtained pursuant to search warrants, I know that Blackshades maintained a customer support forum on its website and had a customer support email address. Customer complaints were opened as "trouble tickets," and would be answered by one of several paid customer service representatives. The Blackshades Server included employee reviews written by Yucel, as well as records reflecting payments made to employees.

25. Records obtained from various electronic payment processors show that Blackshades generated sales of more than $350,000 between September 2010 and April 2014.

The FBI's Identification of Blackshades Users and Seizure of Domains Used to Control Victim Computers

26. According to information provided by CW-1, customers who wished to use the RAT were required to set up an account with Blackshades that included a username and password. In addition, to deploy the RAT, each Blackshades customer was required to

determine how his victims' computers would communicate with his computer. Typically, RAT users set up their accounts so that their victims' computers would communicate with a particular domain name, such as www.example.com. That domain name, in turn, was associated with the IP address of the RAT user's computer through the Domain Name System, or DNS.[4]

27. According to CW-1, when a Blackshades customer set up the RAT, the Blackshades Server logged the domain name to which that customer directed his victims' computers. This information was maintained in one or more database tables on the Blackshades Server. As indicated above, the Government seized a copy of the Blackshades Server pursuant to a search warrant. The copy of that server contained database tables that reflected the usernames and passwords associated with Blackshades accounts, as well as the domain names to which Blackshades users directed their victims' computers.

28. Records obtained from the Blackshades Server and other documents showed that there were more than 6,000 Blackshades customer accounts.[5] Based on information users provided to Blackshades, those users were located in more than 100 countries.

29. As part of the Government's investigation, the Government obtained a court order authorizing the seizure of more than 1,900 domain names used by certain Blackshades customers to control infected computers. By doing so, the FBI disabled communications between those infected computers and the RAT users that had infected them. The court order also authorized the FBI to obtain IP address information for computers trying to communicate with the seized domain names, to enable the FBI to identify and facilitate notification to victims regarding the infections.

FEDOREK's Purchase and Use of the Blackshades RAT

30. In or about February 2013, the Government obtained a warrant to search the email account blackshadessupport@hotmail.com (the "Blackshades Email Account"),

---

[4] Based on my training and experience, I know that DNS is the system through which an easily memorable domain name (e.g., www.doj.gov) is translated - or "resolved" - into an IP address (e.g., 149.101.1.3), thus allowing information to be transmitted between computers.

[5] The number of customer accounts does not necessarily reflect the number of unique users, because a single user could have maintained multiple accounts.

which was used by Yucel to, among other things, communicate with Blackshades employees. The Government's search of the Blackshades Email Account also revealed communications with and/or concerning Blackshades customers, including: (1) email correspondence to and from customers seeking technical support for Blackshades products and services, and (2) electronic receipts reflecting purchases of Blackshades products and services by customers. Those electronic receipts sometimes contained contact information for the Blackshades customer, including email address information.

31. One of the emails I reviewed pursuant to the email search warrant described above was an email dated September 12, 2012, sent from an electronic payment processor (the "Payment Processor") to the Blackshades Email Account. That email shows, among other things, that:

a. On or about September 12, 2012, "Kyle Fedorek" purchased "Blackshades Remote Controller (R.A.T)" for "40.00 USD."

b. FEDOREK provided the Payment Processor an address of a residence in Stony Point, New York as his address (the "FEDOREK RESIDENCE").

32. Pursuant to the search of the Blackshades Server described above, the FBI recovered a database table reflecting the domain names used by Blackshades customers to control their victims' computers. That database table indicated that the user "KBello" had set up several copies of the RAT to communicate with various domain names, including kbella.zapto.org and kbello.zapto.org. Based on records obtained pursuant to subpoena, I have determined that the IP addresses to which those domain names resolved in April and May 2013 were subscribed to the FEDOREK RESIDENCE.

33. On or about March 6, 2014, the Government obtained a search warrant for the FEDOREK RESIDENCE. On or about March 7, 2014, other agents and I executed the warrant and seized a laptop computer from the bedroom of KYLE FEDOREK, the defendant. That laptop had the username "Kyle" and, according to a relative of FEDOREK, the laptop belonged to FEDOREK. A search of FEDOREK's laptop revealed the following:

a. FEDOREK's laptop contained a copy of the Blackshades RAT. The RAT was configured and operating on FEDOREK's laptop. Among other things, the RAT's "form grabber" feature was configured to search for financial account

information. The files recovered from FEDOREK's laptop revealed that he had deployed the form grabber on at least 400 victims.

b. FEDOREK's laptop contained various other forms of malicious software, including the code for viruses that target banking information (such as Carberp and Citadel); code for "phishing" websites - that is, websites designed to look like legitimate sites for financial entities such as banks and credit card companies but which in fact capture victims' personal identification information; electronic publications on how to hack computers; various tools that can be used to spread malware and to prevent its detection by anti-virus software; and BIN files - that is, files that can reveal what bank issued a particular credit card, thereby enabling its exploitation.

c. FEDOREK's laptop contained at least 9,000 usernames and passwords for others' accounts, including login information for electronic payment processors, banks, email accounts, and social networking sites.

d. FEDOREK's laptop contained a file labeled "CreditCardsHackedByNuclearGroup." The file contained what appear to me to be approximately 50,000 credit card numbers, expiration dates, and security codes known as credit card verification numbers, or "CCVs."

e. FEDOREK's laptop contained files that appear to have been exfiltrated from victims' computers. Among other things, it appears that FEDOREK stole personal photographs that were stored on victims' computers. These photographs were contained in a main folder labeled "downloads," and each victim's photographs were contained in a separate subfolder listing the name of the victim's computer.

f. FEDOREK's laptop contained a folder labeled "work." Within that folder were several subfolders whose labels and contents confirmed FEDOREK's involvement in computer hacking activities including, among others:

i. A folder labeled "Bots + Keyloggers." Within that folder were several programs that operate as keyloggers as well as copies of malicious executable files.

ii. A folder labeled "Andromeda v2.06." Based on my training and experience, I know that Andromeda is a program that can be used to spread malware.

iii. A folder labeled "Citadel." Based on my training and experience, I know that Citadel is a virus that is designed to steal victims' banking information.

iv. A folder labeled "Dos + DDoSers" which contained a DDoS tool.

v. A folder labeled "Havij." Based on my training and experience, I know that Havij is a program that can be used to launch cyber attacks known as SQL injections. The folder contained a copy of the program, among other things.

vi. A folder labeled "PHISH SITES." Based on my training and experience, I know that "phishing" refers to schemes in which users are tricked into clicking on a link and/or divulging their confidential personal information. For instance, a phishing website could be created to look like the legitimate website of a bank. Victims directed to the website are thus tricked into entering their username and password to log in to the site. In truth and in fact, their username and password instead is captured by the operator of the phishing site for later exploitation. The folder on FEDOREK's laptop contained files for phony websites for a bank, a credit card company, and an electronic payments processor.

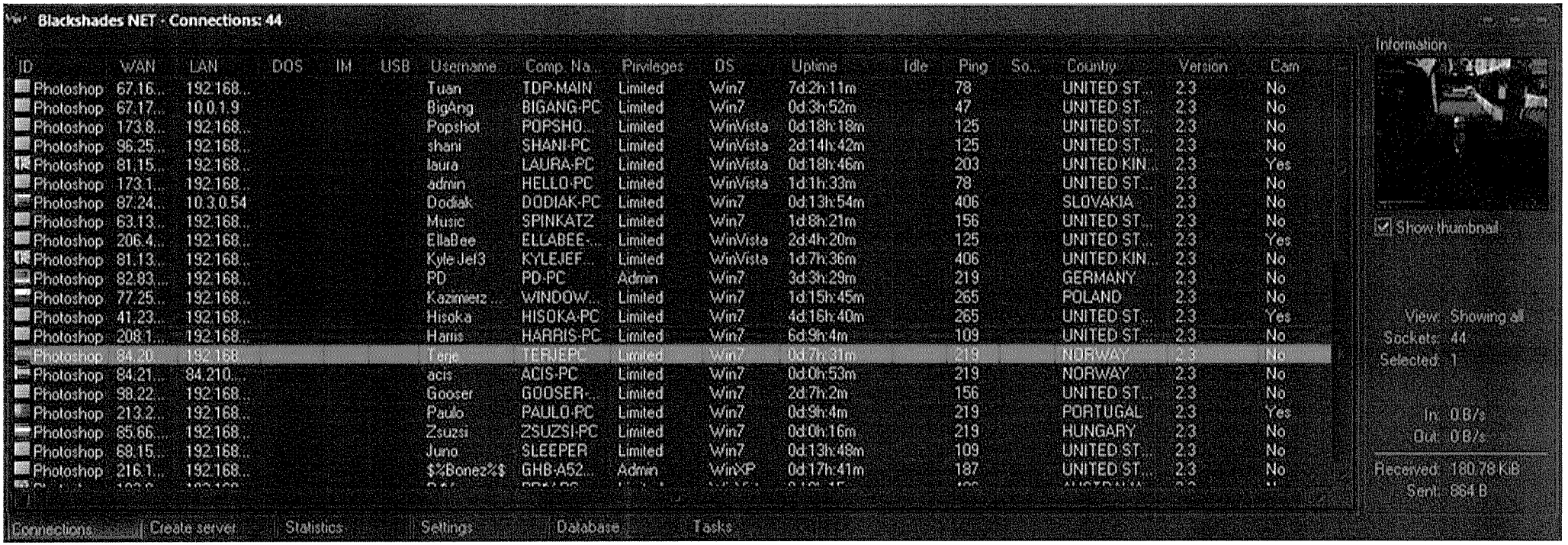
WHEREFORE, I respectfully request that an arrest warrant be issued for KYLE FEDOREK, a/k/a "kbello," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.

NAVIN KALICHARAN
Special Agent
Federal Bureau of Investigation

Sworn to before me this
15th day of May 2014

HON. DEBRA FREEMAN
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

EXHIBIT A


Blackshades NET - Connections: 44
ID WAN LAN DOS IM USB Username Comp. Na... Pirvileges OS Uptime Idle Ping So... Country Version Cam
Photoshop 67.16... 192.168... Tuan TDP-MAIN Limited Win7 7d:2h:11m 78 UNITED ST... 2.3 No
Photoshop 67.17... 10.0.1.9 BigAng BIGANG-PC Limited Win7 0d:3h:52m 47 UNITED ST... 2.3 No
Photoshop 173.8... 192.168... Popshot POPSHO... Limited WinVista 0d:18h:18m 125 UNITED ST... 2.3 No
Photoshop 96.25... 192.168... shani SHANI-PC Limited WinVista 2d:14h:42m 125 UNITED ST... 2.3 No
Photoshop 81.15... 192.168... laura LAURA-PC Limited WinVista 0d:18h:46m 203 UNITED KIN... 2.3 Yes
Photoshop 173.1... 192.168... admin HELLO-PC Limited WinVista 1d:1h:33m 78 UNITED ST... 2.3 No
Photoshop 87.24... 10.3.0.54 Dodiak DODIAK-PC Limited Win7 0d:13h:54m 406 SLOVAKIA 2.3 No
Photoshop 63.13... 192.168... Music SPINKATZ Limited Win7 1d:8h:21m 156 UNITED ST... 2.3 No
Photoshop 206.4... 192.168... EllaBee ELLABEE-... Limited WinVista 2d:4h:20m 125 UNITED ST... 2.3 Yes
Photoshop 81.13... 192.168... Kyle Jel3 KYLEJEF... Limited WinVista 1d:7h:36m 406 UNITED KIN... 2.3 No
Photoshop 82.83... 192.168... PD PD-PC Admin Win7 3d:3h:29m 219 GERMANY 2.3 No
Photoshop 77.25... 192.168... Kazimierz ... WINDOW... Limited Win7 1d:15h:45m 265 POLAND 2.3 No
Photoshop 41.23... 192.168... Hisoka HISOKA-PC Limited Win7 4d:16h:40m 265 UNITED ST... 2.3 Yes
Photoshop 208.1... 192.168... Harris HARRIS-PC Limited Win7 6d:9h:4m 109 UNITED ST... 2.3 No
Photoshop 84.20... 192.168... Terje TERJE-PC Limited Win7 0d:7h:31m 219 NORWAY 2.3 No
Photoshop 84.21... 84.210... acis ACIS-PC Limited Win7 0d:0h:53m 219 NORWAY 2.3 No
Photoshop 98.22... 192.168... Gooser GOOSER-... Limited Win7 2d:7h:2m 156 UNITED ST... 2.3 No
Photoshop 213.2... 192.168... Paulo PAULO-PC Limited Win7 0d:9h:4m 219 PORTUGAL 2.3 Yes
Photoshop 85.66... 192.168... Zsuzsi ZSUZSI-PC Limited Win7 0d:0h:16m 219 HUNGARY 2.3 No
Photoshop 69.15... 192.168... Juno SLEEPER Limited Win7 0d:13h:48m 109 UNITED ST... 2.3 No
Photoshop 216.1... 192.168... $%Bonez%$ GHB-A52... Admin WinXP 0d:17h:41m 187 UNITED ST... 2.3 No
Information
Show thumbnail
View: Showing all
Sockets: 44
Selected: 1
In: 0 B/s
Out: 0 B/s
Received: 180.78 KiB
Sent: 864 B
Connections
Create server
Statistics
Settings
Database
Tasks