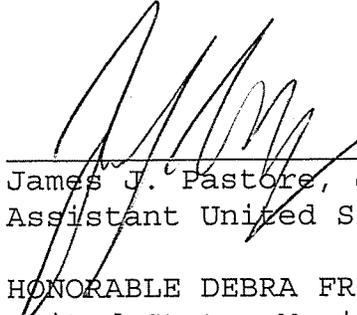


Approved:


James J. Pastore, Jr.
Assistant United States Attorney

14 MAG

1065

Before:

HONORABLE DEBRA FREEMAN
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

MARLEN RAPPA,
a/k/a "nelram,"

:
: COUNTY OF OFFENSE:
: New York

Defendant.

----- x
SOUTHERN DISTRICT OF NEW YORK, ss.:

SAMAD D. SHAHRANI, 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 February 29, 2012, up to and including in or about March 2014, in the Southern District of New York and elsewhere, MARLEN RAPPA, a/k/a "nelram," 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 MARLEN RAPPA, a/k/a "nelram," 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, RAPPA 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, steal their personal files, and spy on them.

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 February 29, 2012, MARLEN RAPPA, a/k/a "nelram," the defendant, 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 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 February 29, 2012, up to and including in or about March 2014, in the District of New Jersey and elsewhere, MARLEN RAPPA, a/k/a "nelram," 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, RAPPA used malicious software, or malware, including Blackshades malware, to infect victims' computers, steal their personal files, and spy on them.

(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:

5. 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.

6. I have been a Special Agent with the FBI since approximately September 2011. Since approximately October 2012, 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

7. 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.

8. 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.

9. MARLEN RAPPA, a/k/a "nelram," the defendant, was a customer of Blackshades who purchased the RAT in or about February 2012. From in or about February 2012 through in or about March 2014, when the FBI executed a search warrant at RAPPA's residence and seized his computer, RAPPA used the RAT to infect victims' computers, spy on those victims using their web cameras, and steal personal files from their computers. As detailed below, the search of RAPPA's computer showed that RAPPA was also deploying a variety of other types of malicious software against his victims.

Background on the Blackshades RAT

10. 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 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 -

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.

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."

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.

11. 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.

12. 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 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).

13. 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:

IP	WAN	LAN	OS	IM	USB	Username	Comp. No.	Platform	OS	Update	Mem	Log	Ex.	Country	Version	Cam
PhotoShop	67.16.	192.168.				Tuan	TDP.H4M	Limited	Win7	7/3/2010	78			UNITED ST.	2.3	No
PhotoShop	67.17.	16.0.1.9				Bigling	DINGNG.FC	Limited	Win7	6/12/2010	47			UNITED ST.	2.3	No
PhotoShop	173.8	192.168.				Popolnot	POPSHO	Limited	WinVista	6/11/2010	157			UNITED ST.	2.3	No
PhotoShop	55.25	192.168.				lyant	SHARP.FC	Limited	WinVista	2/11/2010	157			UNITED ST.	2.3	No
PhotoShop	81.15	192.168.				Isma	LAPRAF	Limited	WinVista	6/11/2010	207			UNITED ST.	2.3	Yes
PhotoShop	173.1	192.168.				shim	HELLO.FC	Limited	Win7	1/11/2010	78			UNITED ST.	2.3	No
PhotoShop	87.24.	192.168.				Bobak	BOBOK.FC	Limited	Win7	6/11/2010	405			SLOVAKIA	2.3	No
PhotoShop	63.10.	192.168.				Mario	SPHOKALZ	Limited	Win7	1/8/2010	157			UNITED ST.	2.3	No
PhotoShop	205.4.	192.168.				Ethias	ELUDEE	Limited	WinVista	2/4/2010	157			UNITED ST.	2.3	Yes
PhotoShop	81.13.	192.168.				KyleJrB	KYLEJFB	Limited	WinVista	1/7/2010	406			UNITED ST.	2.3	No
PhotoShop	82.93.	192.168.				FD	PO.FC	Limited	Win7	2/2/2010	219			GERMANY	2.3	No
PhotoShop	77.25.	192.168.				Katowez	WINGOW	Limited	Win7	1/15/2010	255			POLAND	2.3	No
PhotoShop	41.22	192.168.				Hedra	HISOKA.FC	Limited	Win7	4/18/2010	355			UNITED ST.	2.3	Yes
PhotoShop	238.1.	192.168.				Hest	HAFRIS.FC	Limited	Win7	6/29/2010	109			UNITED ST.	2.3	No
PhotoShop	81.20.	192.168.				Tana	TERNEP	Limited	Win7	6/7/2010	219			NORWAY	2.3	No
PhotoShop	81.21.	81.210.				ad.	ACIS.FC	Limited	Win7	6/16/2010	219			NORWAY	2.3	No
PhotoShop	53.22	192.168.				Gooset	GOOSER	Limited	Win7	2/7/2010	156			UNITED ST.	2.3	No
PhotoShop	3132	192.168.				Paulo	PAULO.FC	Limited	Win7	0/28/2010	219			PORTUGAL	2.3	Yes
PhotoShop	85.65	192.168.				Zauri	ZHAUSI.FC	Limited	Win7	6/10/2010	219			HUNGARY	2.3	No
PhotoShop	69.15.	192.168.				Juno	SLESPEE	Limited	Win7	6/11/2010	109			UNITED ST.	2.3	No
PhotoShop	215.1.	192.168.				3-Bene	DHEA52	Limited	Win7	6/17/2010	187			UNITED ST.	2.3	No

Among other things, the user interface³ 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.

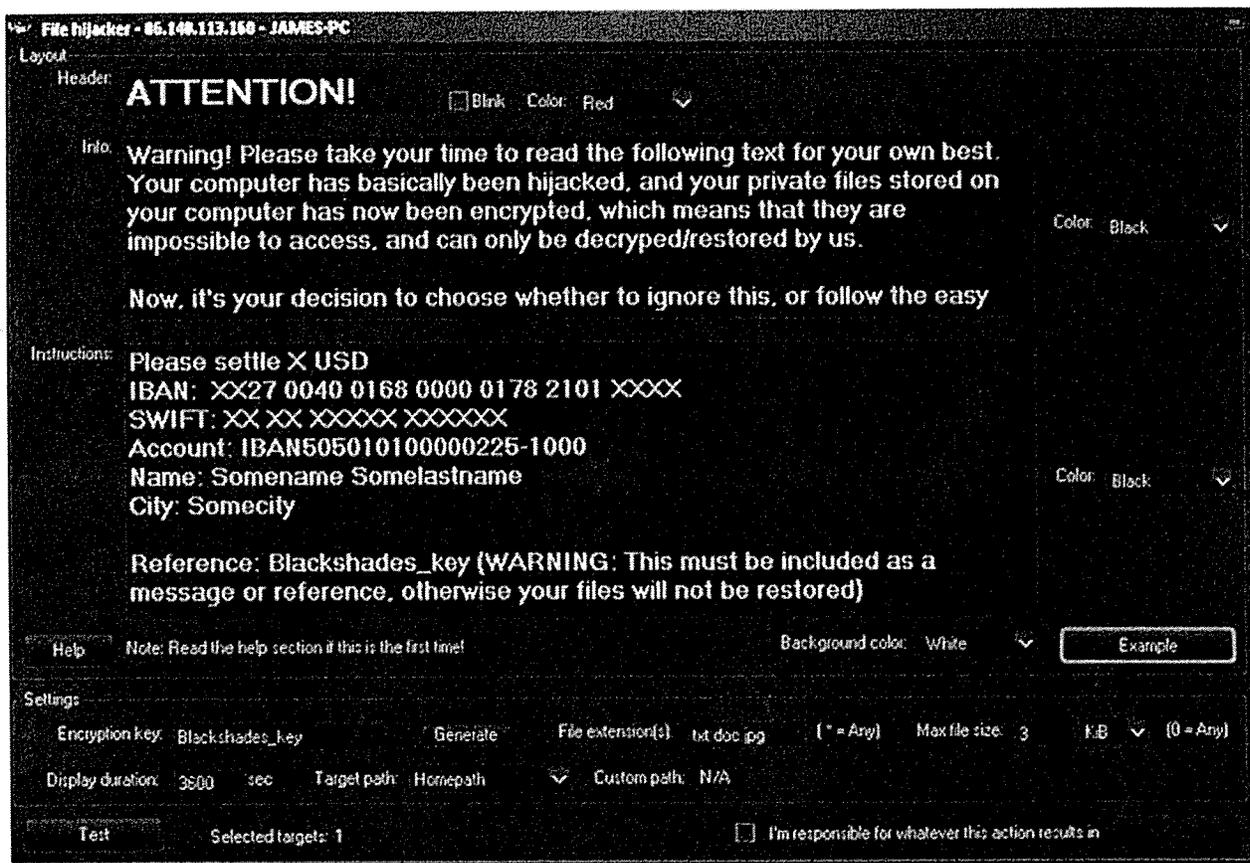
14. Once a computer was infected with the RAT, the user of the RAT could remotely activate the victim's web camera. By doing so, the RAT user could take photographs or obtain a live feed from the infected computer's web camera. In this way, the user could spy on anyone within view of the victim's webcam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

15. The RAT also contained a "keylogger" feature that allowed users to record each key that victims typed on their

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

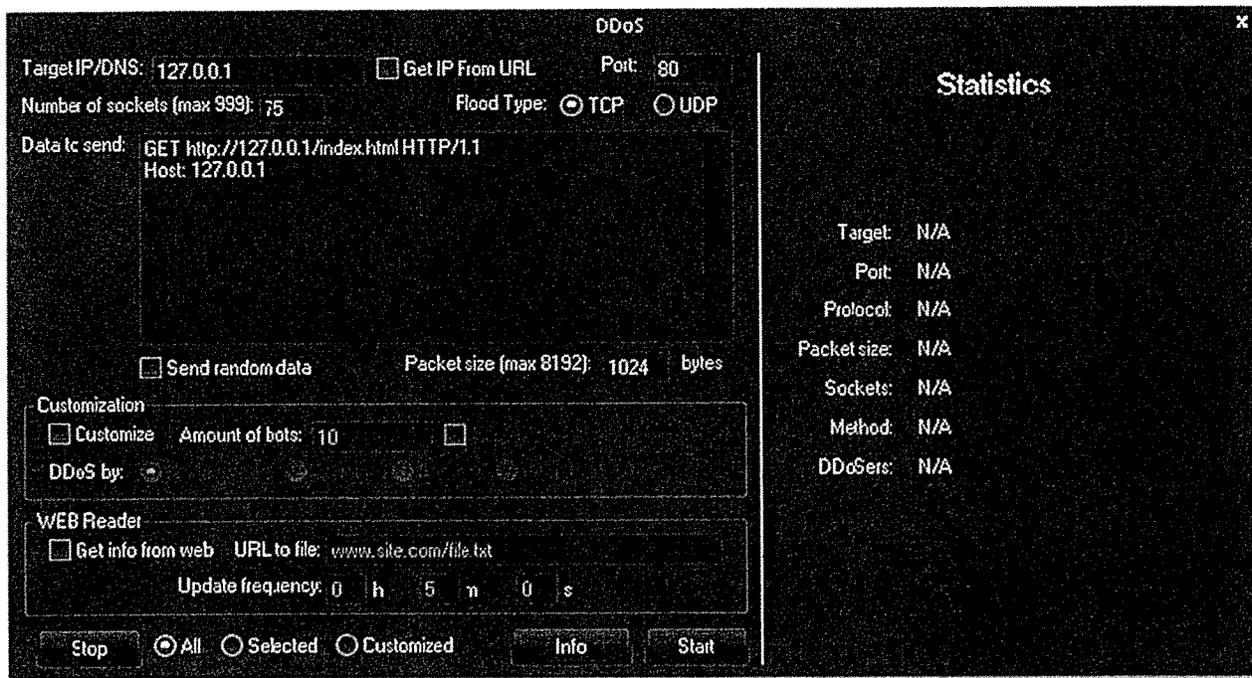
computer keyboards. To help users steal a victim's passwords and other log-in credentials, the RAT also had a "form grabber" feature. The "form grabber" automatically captured log-in information that victims entered into "forms" on their infected computers (e.g., log-in screens or order purchase screens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

16. 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:



17. 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:



18. 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

19. 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.

20. 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.

21. 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

22. 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.

23. 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.

24. 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

25. 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

26. 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.

27. 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.

28. 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

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 maintain multiple accounts.

identify and facilitate notification to victims regarding the infections.

RAPPA's Purchase and Use of the Blackshades RAT

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

30. One of the emails I reviewed pursuant to the email search warrant described above was an email dated February 29, 2012, sent from an electronic payment processor (the "Payment Processor") to the Blackshades Email Account. That email shows that:

a. On or about February 29, 2012, "Marlen Rappa" purchased "Blackshades Remote Controller (R.A.T)" for "40.00 USD."

b. The customer who purchased the RAT provided the email address bayshoreim@gmail.com to the Payment Processor, and was using a particular IP address ending in .88.

31. According to records obtained from Google for the email account bayshoreim@gmail.com, that account was created on or about January 19, 2012, from the same IP address used to purchase the RAT. The email account was subscribed to in the name "Marlen R." with a phone number ending in 5761 (the "5761 Phone"). In addition, throughout May 2013, the email account repeatedly was accessed from a particular IP address ending in .194, among others. According to subscriber records for that IP address, during May 2013, that IP address was subscribed to an account with an address in Middletown Township, New Jersey (the "RAPPA Residence") and listed the 5761 Phone as an associated phone number (i.e., the same phone number associated with the Google account for email address bayshoreim@gmail.com).

32. In or about March 2014, other agents and I executed a search warrant at the RAPPA Residence and recovered, among other

things, a computer from the garage (the "Computer"). MARLEN RAPPA, a/k/a "nelram," the defendant, stated that he had the Computer for approximately six years and that no one else had access to it.

33. A search of the Computer revealed a folder entitled "Blackshades," which contained approximately seven versions of the Blackshades RAT. A search of that folder showed that RAPPA had used the Blackshades RAT to spy on and steal files and other information from multiple victims from in or about March 2012 through in or about February 2014. Specifically, RAPPA had used the RAT to spy on and secretly capture images of at least 45 victims through their computers' web cameras. In addition, RAPPA had used the Blackshades malware to steal electronic files, including videos and photographs, from approximately 95 victim computers. The stolen photographs included sexually explicit images. RAPPA had installed the Blackshades keylogger on at least 35 victim computers.

34. The search of the Computer also revealed that MARLEN RAPPA, a/k/a "nelram," the defendant, used a variety of other hacking tools. For example, the Computer also contained:

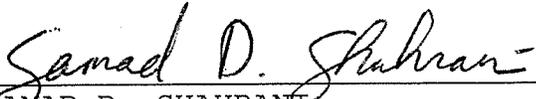
a. A folder named "Dark Comet 5.2," which, from my training and experience, I know to be another brand of remote access tool;

b. Other folders that appeared to contain remote access tools, including JRAT, Sharpeye RAT, Pocket RAT, Cerberus RAT, Xtreme RAT, and Syla RAT;

c. A file containing instructions for hacking into remote computers; and

d. A folder named "spreading guide," which appeared to contain instructions for installing remote access tools on victim computers.

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


SAMAD D. SHAHRANI
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	WAIN	DOS	IM	USB	Username	Comp. Na.	Privileges	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...			Isaura	LAURA-PC	Limited	WinVista	0d 18h 45m		203		UNITED KIN...	2.3	Yes
Photoshop	173.1...	192.168...			adnan	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...			Kazmercz	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	84.21...	192.168...			Legie	TERJEP	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...			Goosier	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	68.15...	192.168...			Juno	SLEEPER	Limited	Win7	0d 13h 48m		109		UNITED ST...	2.3	No
Photoshop	216.1...	192.168...			\$\$Bomez\$\$	GHB-452...	Admin	WinXP	0d 17h 41m		187		UNITED ST...	2.3	No



Show thumbnail

View: Showing all
Sockets: 44
Selected: 1

In: 0B/s
Out: 0B/s

Received: 180.78 KiB
Sent: 884 B