1523

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 15-153
	)	
NAVEED AHMED	)	
a/k/a "Nav"	)	(18 U.S.C. § 371)
a/k/a "semaph0re"	)	
PHILLIP R. FLEITZ	)	
a/k/a "Strife"	)	
DEWAYNE WATTS	)	
a/k/a "m3t4lh34d"	)	
a/k/a "metal"	)	

INFORMATION

INTRODUCTION

At all times relevant to the INFORMATION:

1. DARKODE was an Internet forum where individuals convened online to buy, sell, trade, and discuss intrusions on others' computers and electronic devices. One could only become a member of DARKODE by declaring to existing members what type of relevant ability or product they could bring to the forum and then being approved for membership by the other members.

2. Defendant NAVEED AHMED resided in the state of Florida and used the Internet nicknames "Nav" and "semaph0re." AHMED was a member of the Internet forum known as DARKODE.

3. Defendant PHILLIP R. FLEITZ resided in the state of Indiana and used the Internet nickname "Strife."

4. Defendant DEWAYNE WATTS resided in the state of Florida and used the Internet nicknames "m3t4lh34d" and "metal." WATTS had an account on the Internet forum known as DARKODE.

5. "SMS" is the acronym for "short message service" which is a text messaging service component of phone, Web, or mobile communications systems.

COUNT ONE

The United States Attorney charges:

THE CONSPIRACY AND ITS OBJECTS

6. From in and around September 2011, and continuing thereafter until on or about February 28, 2013, in the Western District of Pennsylvania and elsewhere, the defendants, NAVEED AHMED, a/k/a "Nav," a/k/a "semaph0re", PHILLIP R. FLEITZ, a/k/a "Strife," and DEWAYNE WATTS, a/k/a "m3t4lh34d," a/k/a "metal", knowingly and willfully did conspire, combine, confederate and agree together and with each other, and with other persons known and unknown to the grand jury, to commit offenses against the United States, that is:

a) Knowingly, in or affecting interstate or foreign commerce, using a protected computer to relay or retransmit multiple commercial electronic mail messages with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages, and the volume of the electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during

any 1-year period; and as a result of the offense any individual committing the offense obtained anything of value aggregating $5,000 or more during any 1-year period, in violation of Title 18, United States Code, Section 1037(a)(2) and (b)(2)(C), (b)(2)(E).

MANNER AND MEANS OF THE CONSPIRACY

7. It was a part of the conspiracy that the conspirators would control two servers at a "bullet-proof hoster" based in China (hereinafter "the China servers") which would execute programs that scanned Internet-connected routers usually located in developing countries.

8. It was further a part of the conspiracy that once a vulnerable router was detected by the China servers, the China servers would access the routers without authorization and download and install proxy-server software onto the router which infected the router (hereinafter "the infected routers") and placed the router under the control of the conspirators for the purpose of using the router as a proxy computer to mail commercial email messages while masking the true origin of the messages.

9. It was further a part of the conspiracy that the conspirators controlled servers in the United States (hereinafter "the mailing servers") which were used to initiate the mailing of the commercial email messages by the conspirators.

10. It was further a part of the conspiracy that the conspirators would use a program which would generate a random list

of millions of phone numbers, including those belonging to users in the Western District of Pennsylvania, and turn them into email addresses by adding the appropriate SMS provider domain to the phone number. These email messages were intended to be sent to victim phones as SMS messages.

11. It was further a part of the conspiracy that the conspirators would create SMS-style messages which would offer a free Best Buy gift card and contain weblinks to domains controlled by the conspirators. These domains were crafted by the conspirators to escape spam filters maintained by the SMS providers and were purchased with prepaid debit cards or other anonymous means of payment, and registered with false information, so as to hide the identity of the conspirators.

12. It was further a part of the conspiracy that the mailing servers would pair the created SMS messages with the generated email addresses and mail millions of messages to the infected routers. The infected routers, in turn, would forward the messages to the indicated generated email addresses as SMS messages, including those based in the Western District of Pennsylvania.

Thus, the SMS messages would appear to SMS providers as having originated from the infected routers rather than the mailing servers.

13. It was further a part of the conspiracy that victim cell phones, including those in the Western District of Pennsylvania, would receive the SMS messages generated by the conspirators.

14. It was further a part of the conspiracy that if the users of the victim cell phones "clicked" the weblink within the SMS message sent by the conspirators, those victims would be directed to a website (known as the "landing page") controlled by the conspirators before being redirected to another website (known as the "affiliate page") upon the entry of a provided "access code."

15. It was further a part of the conspiracy that the conspirators would enter into a contractual relationship with an Internet Cost Per Action network (CPA), who controlled the "affiliate page," in which they would derive income for each bit of personal information, such as e-mail accounts, provided by the victim user(s).

16. It was further a part of the conspiracy that the conspirators would direct the CPA to place the proceeds of this scheme into a bank account in Switzerland controlled by an unindicted co-conspirator. The unindicted co-conspirator would then wire the proceeds to the conspirators in the U.S., or to their U.S.-based bank accounts, but only after keeping 10% of the proceeds for laundering them.

OVERT ACTS

17. In furtherance of the conspiracy, and to effect the objects of the conspiracy, the defendants, NAVEED AHMED, a/k/a "Nav," a/k/a "semaph0re," PHILLIP R. FLEITZ, a/k/a "Strife," and DEWAYNE WATTS, a/k/a "m3t4lh34d," a/k/a "metal", and with others both known and unknown to the grand jury, did commit and cause to be committed, the

following overt acts, among others, in the Western District of Pennsylvania and elsewhere:

(a) On or about December 3, 2012, the conspirators caused to be delivered an SMS message to 412-735-****, which stated "Congratulations, your 4-th place code is: H7G0 www.BestBuyVouchers.com."

(b) On or about December 5, 2012, the conspirators caused to be delivered an SMS message to 412-304-****, which stated "Congratulations! You've finished Fifth! Your Code is: WM154 www.FreeBestBuyCards.net".

(c) On or about December 27, 2012, the conspirators caused to be delivered an SMS message to 412-804-****, which stated "Your entry placed 8 out of 10! Claim the prize with this Code: U0V2 www.BBCodeTexts.net."

In violation of Title 18, United States Code, Section 371.

DAVID J. HICKTON
UNITED STATES ATTORNEY
PA ID No. 34524