

1523

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

UNITED STATES OF AMERICA)	
)	Criminal No. 15-154
v.)	
)	18 U.S.C. §§ 1037(a)(1),
)	(b)(2)(A), and 2
ERIC L. CROCKER,)	
a/k/a "Phastman")	

INFORMATION

INTRODUCTION

At all times relevant to this 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 he or she could bring to the forum and then being approved for membership by the other members.

2. The "Facebook Spreader" was computer code that was featured on the DARKODE forum and was created to infect large numbers of computers through the use of the social media platform Facebook. Once the Facebook Spreader infected a victim's computer, the malware would access the victim's Facebook account, then the victim's Facebook "friends" list, and then send out spearphishing messages to each of the victim's Facebook friends, purporting to be from the victim. If the recipient of the message clicked the weblink included within the message, a computer file would be downloaded onto the

recipient's computer. When the recipient opened the computer file, the recipient's computer was then infected with malware known as "Slenfbot" and/or "Dolbot."

3. "Slenfbot" and/or "Dolbot" was "loader" malware which, when downloaded and installed onto a victim computer, would "call back" over the Internet to "command and control" computer servers controlled by ERIC L. CROCKER and others to download the Facebook Spreader onto the recipient computer and the process would continue to the new victim's Facebook friends list.

4. The "command and control" servers used by ERIC L. CROCKER belonged to unknowing third parties, and were hacked by the ERIC L. CROCKER and others. The servers enabled ERIC L. CROCKER and others to connect to and control the infected computers as a botnet.

5. The defendant, ERIC L. CROCKER, and others would sell access to the Facebook Spreader/Slenfbot botnet to an unidentified coconspirator who would utilize the infected computers within the botnet to send high volumes of spam messages.

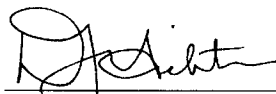
6. The defendant, ERIC L. CROCKER, and others would be paid approximately \$200-300 for every 10,000 active infections by the unidentified coconspirator for maintaining the size of the botnet through the constant use of the Facebook spreader.

COUNT ONE

The United States Attorney charges:

From on or about August 1, 2011, until on or about October 6, 2012, in the Western District of Pennsylvania and elsewhere, the defendant, ERIC L. CROCKER, a/k/a "Phastman," knowingly did aid, abet, and assist others, in and affecting interstate and foreign commerce, and did knowingly access a protected computer without authorization, namely a computer that had been infected by the Facebook Spreader and Slenfbot, and did intentionally initiate the transmission of multiple commercial electronic mail messages from or through such computer.

In violation of Title 18, United States Code, Sections 1037(a)(1), (b)(2)(A) and 2.



DAVID J. HICKTON
United States Attorney
PA ID No. 34524