BRYAN D. SCHRODER
United States Attorney

ADAM ALEXANDER
Assistant U.S. Attorney
Federal Building & U.S. Courthouse
222 West 7th Ave., #9, Rm. 253
Anchorage, AK 99513-7567
Phone: 907-271-5071
Email: adam.alexander@usdoj.gov

KENNETH A. BLANCO
Acting Assistant Attorney General

CATHERINE ALDEN PELKER
Trial Attorney
Computer Crime & Intellectual Property Section
1301 New York Avenue, NW, Suite 600
Washington, DC 20005
Telephone: (202) 514-1026
Facsimile: (202) 514-6113
Email: Catherine.Pelker@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA,	)	No.
	)	
Plaintiff,	)	COUNT 1:
	)	CONSPIRACY TO COMMIT A
vs.	)	VIOLATION OF 18 U.S.C. § 1030(a)(5)
	)	Vio. Of 18 U.S.C. § 371
PARAS JHA,	)	
	)	
	)	
Defendant.	)	

INFORMATION

The United States Attorney charges that:

INTRODUCTION

1. The "Internet" is a global network connecting millions of computers and computer networks to each other, allowing them to communicate and transfer information. Using, among other things, a system of wires, cables, routers and circuits, the Internet allows the communication and transfer of information in interstate and foreign commerce. Computers that are connected to the Internet may come in different forms, from personal computers, laptops and smartphones, to large-scale servers that host websites and online services, to more minimal devices such as Internet-connected cameras, digital video recorders ("DVR") and routers.

2. "Malware" is malicious software designed to damage or disable a computer, or provide control of the computer to a third party.

3. A "botnet" is a collection of computers infected with malware that are controlled as a group, typically without the owners' knowledge. The individual computers within a botnet, known as "bots," respond to commands from one or more master computers. These master computers are commonly known as "command and control" ("C2") computers.

4. A "proxy" is an intermediary computer server that relays traffic from one computer to another. Proxies are used to obfuscate the Internet Protocol address of the originating computer, which makes online attribution more difficult.

5. "Clickfraud" is a type of Internet-based fraud scheme that utilizes "clicks," or the accessing of web addresses and similar web content, for the purpose of artificially generating revenue. Clickfraud capitalizes on the common internet advertising payment

model in which advertisers pay based on the total number of times their advertisement is viewed (per-per-impression) or based on the total number of times their advertisement is "clicked" (pay-per-click). Clickfraud involves fraudulently generating clicks or views, causing the advertiser to substantially increase their payouts, which generates profits for the Clickfraud perpetrators.

COUNT 1 (Conspiracy)

6. The allegations set forth in paragraphs one through five of this Information are re-alleged as if fully stated herein.

7. Between in or about December 2016, and continuing thereafter to in or about February 2017, in the District of Alaska and elsewhere, defendant PARAS JHA, and other persons, did knowingly and intentionally conspire and agree with one another to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, and to cause damage affecting 10 or more protected computers during a 1-year period in violation of 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(A).

THE OBJECT OF THE CONSPIRACY

8. The object of the unlawful conspiracy was to infect computing devices with malware for the purpose of enlisting those devices into a botnet that could be used to engage in criminal activity, including advertising fraud, and particularly clickfraud.

MANNER AND MEANS OF THE CONSPIRACY

9. It was a part of the conspiracy that the defendant PARAS JHA and his co-conspirators would identify vulnerable computer devices connected to the internet and,

without authorization, attempt to gain administrative access to those devices through the use of credentials that they were not authorized to employ.

10. It was further part of the conspiracy that the defendant PARAS JHA and his co-conspirators would, without authorization, infect those devices with malware, which afforded the defendant PARAS JHA and his co-conspirators complete control over the devices and enlisted the devices into a botnet. JHA and his co-conspirators eventually controlled over 100,000 such devices, including devices located in the District of Alaska.

11. It was further part of the conspiracy that the defendant PARAS JHA and his co-conspirators would design and build the botnet with the intent of using the victim computers in furtherance of advertising fraud schemes, including clickfraud.

12. It was further part of the conspiracy that the defendant PARAS JHA and his co-conspirators would rent access to their botnet, which enabled other criminals to use the botnet to conduct clickfraud.

13. It was further part of the conspiracy that the defendant PARAS JHA and his co-conspirators would transmit commands to the devices controlled by the botnet in order to direct the devices' participation in various criminal schemes, including clickfraud.

14. It was further part of the conspiracy that JHA and his co-conspirators intentionally caused damage to the victim devices while building the botnet and sending commands to the devices. The installation of the malware and subsequent commands all impaired the integrity of the victim devices, and the high volume of web requests associated with the clickfraud activity slowed or degraded at least some of the devices. JHA and his co-conspirators specifically targeted home internet routers associated with a U.S.-based

Internet Service Provider, and the volume of clickfraud activity pushed through the routers limited the amount of bandwidth available to the home consumers.

15. It was further part of the conspiracy that the defendant PARAS JHA and his co-conspirators would obtain value from the botnet and the resulting fraud, in the form of profits from the fraudulent advertising revenue earned through clickfraud activity, botnet rental payment, information, and the use of the computers. As a result of this scheme, Jha and his co-conspirators received as proceeds approximately two hundred bitcoin, valued on January 29, 2017 at over $180,000.

OVERT ACTS

16. In furtherance of the conspiracy and to effect the objects of the conspiracy, the following overt acts, among others, were committed in the District of Alaska and elsewhere:

a. From December 2016 to January 2017, defendant PARAS JHA wrote source code to develop and support the botnet and to enable its clickfraud activities. JHA adapted the code to handle a large number of bots, which eventually exceeded 100,000, allowing JHA and his co-conspirators to capitalize on the availability of a large pool of prospective victim devices and to maximize the size of the botnet. The malicious program developed by JHA and his co-conspirators caused damage to the victim devices.

b. From December 2016 to January 2017, defendant PARAS JHA set up and managed command and control (C2) servers to manage the infected computers. JHA configured his botnet control software to interact with

victim devices so that they could most effectively participate in the clickfraud activities.

c. In or about January 2017, defendant PARAS JHA was a principal point of contact for the clickfraud botnet's main customers. JHA communicated with the clients regarding the botnet and its activities. JHA worked with his co-conspirators to ensure that the victim devices participating in the botnet performed the activities requested by the criminal customers leasing the botnet.

d. In or about January 2017, JHA configured a set of compromised devices to access particular web addresses and associated content, in furtherance of advertising fraud schemes.

e. From December 2016 to January 2017, JHA and his co-conspirators worked to identify private zero-day vulnerabilities, meaning vulnerabilities that had not yet been disclosed. JHA would then configure the botnet to interact with the newly identified victims.

All of which is in violation of Title 18, United States Code, Section 371.

RESPECTFULLY SUBMITTED December 5, 2017, in Anchorage, Alaska.

BRYAN SCHRODER
United States Attorney

s/ Adam Alexander
ADAM ALEXANDER
Assistant U.S. Attorney
United States of America