2015R00240/SW

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Honorable
v.	:	Criminal No. 17-
PARAS JHA	:	18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B)(i), and 2

INFORMATION

The defendant having waived in open court prosecution by Indictment, the Acting United States Attorney for the District of New Jersey charges:

1. At all times relevant to this Information, the following definitions applied:

a. Bot: A bot is an automated computer program that performs specific functions. Bots can perform useful tasks, such as regularly updating weather and traffic conditions on local news websites or scanning the Internet to update comparison shopping websites. Bots also can perform destructive tasks such as scanning the Internet for unsecured computers for the purpose of identifying and sometimes installing computer viruses or other destructive programs. These compromised or "zombie" computers then can be used to repeatedly attack a domain or IP address on behalf of the bot originator or "bot herder."

b. Botnet: A collection of bots is a "robot network" or botnet. A

botnet typically is remotely controlled by the bot herder using a "command and control" server, which is connected to the Internet. A botnet generally is comprised of large numbers of computers.

c. Distributed Denial of Service ("DDoS") Attack": A DDoS attack involves using a large network of computers, commonly a botnet, to flood a victim website with repeated requests for information or "junk" data, which could effectively cripple the site by overloading it with too much information simultaneously. The perpetrators of DDoS attacks gain control of large numbers of computers to use in this type of attack, commonly by assembling a botnet. Once the botnet is in place, when used for a DDoS attack, it is either programmed to attack specific sites or it awaits further instructions from the command and control server.

2. At various times relevant to this Information:

a. Defendant PARAS JHA resided in or near Fanwood, New Jersey.

b. Rutgers, The State University of New Jersey ("Rutgers University"), was a public research university with campuses and facilities throughout New Jersey.

c. Rutgers University operated all its daily business through a computer network known as the central authentication server.

d. The central authentication server was a protected computer system that was connected to the Internet.

e. The central authentication server maintained, among other things, the gateway portal https://sakai.rutgers.edu, through which staff, faculty, and students coordinated, among other things, messaging, online teaching, assignment delivery, and assessment.

3. Between in or about November 2014 and in or about September 2016, Defendant PARAS JHA executed a series of DDoS attacks against Rutgers University by attacking the central authentication server.

4. Defendant PARAS JHA's DDoS attacks effectively shutdown Rutgers University's central authentication server, sometimes for days at a time, causing damage to Rutgers University, its faculty, and its students.

5. From in or about November 2014 through in or about September 2016, in the District of New Jersey and elsewhere, defendant

PARAS JHA

knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, recklessly caused damage without authorization, to a protected computer, and thereby disrupted the availability of Rutgers University's central authentication server, causing more than $5,000 in loss within a one-year period.

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

FORFEITURE ALLEGATION

1. Upon conviction of the offenses in violation of 18 U.S.C. § 1030 alleged in this Information, defendant PARAS JHA shall forfeit to the United States:

a. pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of the offense charged in this Information; and

b. pursuant to 18 U.S.C. § 1030(i), all right, title, and interest of the defendant in any personal property that was used or intended to be used to commit or to facilitate the commission of the offense charged in this Information, including, but not limited to, all right, title, and interest of the defendant in the following:

(a) All the computers, media storage devices, and mobile phones listed in Schedule B that were seized pursuant to a search warrant on or about January 18, 2017.

SUBSTITUTE ASSETS PROVISION

2. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

the United States shall be entitled, pursuant to 21 U.S.C. § 853(p) (as incorporated by 28 U.S.C. § 2461(c), 18 U.S.C. § 1030(i), and 18 U.S.C. § 982(b)), to forfeiture of any other property of the defendant up to the value of the above-described forfeitable property.

WILLIAM E. FITZPATRICK
ACTING UNITED STATES ATTORNEY