Source:
http://www.nj.com/education/2017/12/
rutgers_student_charged_in_series_of_cyber_attacks.html#incart_river_home

nj com True Jersey.

Former Rutgers student admits to creating code that crashed internet

Updated Dec 13;
Posted Dec 13

Former Rutgers University student Paras Jha, left, leaves the U.S. District Courthouse in Trenton with his attorney, Robert Stahl, on Wednesday, Dec. 13, 2017. (Jeff Granit | For NJ.com)

By **Kelly Heyboer and Ted Sherman**

NJ Advance Media for NJ.com

A former Rutgers University student has pleaded guilty in federal court to being one of the architects of a computer virus that crashed websites around the world in October 2016 in one of the worst outages in the history of the internet, prosecutors said.

Paras Jha, of Fanwood, also pleaded guilty in federal court in Trenton Wednesday to an additional computer fraud charge for repeatedly disabling Rutgers University's internet network while taunting school officials on social media.

His attorney said Jha is sorry for what he did and takes full responsibility for his actions.

"Paras Jha is a brilliant young man whose intellect and technical skills far exceeded his emotional maturity," said Robert Stahl, Jha's attorney.

The 21-year-old former Rutgers computer science major, who lives at home with his parents, admitted in a series of pleas that stretch from New Jersey to Alaska to helping create powerful computer codes, including the "Mirai" computer virus that terrorized the internet in 2016.

He and his co-conspirators used the code to crash various websites, then published the "Mirai" virus on hacker websites in September 2016, prosecutors said. The following month, other hackers took the code and launched a massive cyber attack that crippled much of the internet.

Though his code was used, Jha is not charged with directly launching the October 2016 cyber attack that crashed Twitter, Netflix and other websites around the world, prosecutors said. Those hackers remain unknown and investigators declined to comment on the investigation.

On Wednesday morning, standing before U.S. District Judge Michael Shipp in federal court in Trenton dressed in a dark suit and dark-rimmed glasses, Jha admitted to repeatedly crashing Rutgers' computer network between 2014 and 2016. He said he bragged about his exploits online using the screen name "exfocus".

Jha admitted to timing his attacks on Rutgers' websites to when they would cause the most disruption to students, faculty and staff.

"In fact, you timed your attacks because you wanted to overload the central authentication server when it would be the most devastating to Rutgers, right?" Assistant U.S. Attorney Shana Chen asked Jha in court.

"Yes," he said in a clear, strong voice.

Jha gave no motive for his attacks on Rutgers or his attacks on the internet.

He faces up to 10 years in prison, though he will likely face far less prison time under federal sentencing guidelines. He also faces a $250,000 fine and has agreed to forfeit 13 bitcoin -- worth about $221,000 -- as restitution.

Jha was released on a $25,000 bond. He is scheduled to be sentenced Mar. 13.

Rutgers officials said they were pleased the individual who repeatedly crashed the university's servers and cut off the internet to thousands of students, faculty and staff for days at a time has been caught. The university spent more than $3 million upgrading its cyber security during the attacks.

"We hope the results of this investigation demonstrate how seriously we take such criminal acts and the harm they cause the Rutgers community," Rutgers officials said in a statement.

Two other men -- Josiah White, 20, of Washington, Pennsylvania, and Dalton Norman, 21, of Metairie, Louisiana -- also pleaded guilty Dec. 8 to conspiring with Jha on the wider botnet scheme, according to court papers filed in Alaska.

The "Mirai" botnet worked by creating a collection of computers infected with "malware" software that controls the devices without their owner's knowledge, according to a plea agreement filed Dec. 5 in federal court in Alaska.

The botnet targeted internet-connected devices, known as the Internet of Things, including wireless cameras, routers and digital video recorders.

"Jha and his co-conspirators successfully infected hundreds of thousands of internet-connected computing devices, including computers in Alaska and other states, with malicious software," the plea agreement said.

Investigators opened the case in Alaska because that is where some of the first devices were infected by the "Mirai" botnet virus, which was named after a Japanese anime character Jha and his co-conspirators liked, prosecutors said.

The three men, who met each other online, used the botnet to launch DDoS -- or a distributed denial of service -- attacks that targeted the websites of businesses, rivals or others against whom they "held grudges," court papers said.

The hackers also made money by renting out the botnet to others and by forcing internet hosting companies to pay "protection money" to avoid getting hit with cyber attacks, the plea agreement said.

They also created a separate botnet, which investigators dubbed the "clickfraud" botnet, was used between December 2016 and January 2017 to route internet traffic to unnamed websites, artificially driving up clicks on ads and other content, the court papers said.

Jha and his co-conspirators made more than $180,000 leasing access to the 100,000 computers in the "clickfraud" botnet to other criminals who made money by directing fake internet traffic to ads on the targeted websites, according to the plea agreement.

"The Mirai and Clickfraud botnet schemes are powerful reminders that as we continue on a path of a more interconnected world, we must guard against the threats posed by cybercriminals that can quickly weaponize technological developments to cause vast and varied types of harm," said Acting Assistant Attorney John P. Cronan of the Justice Department's Criminal Division.

Jha is well-known in the cyber security world. The former Rutgers computer science student was previously accused by a prominent cyber security blogger of being the author of the "Mirai" botnet code that caused the massive Oct. 21, 2016, internet outage.

In that case, botnets took down Twitter, Netflix, Reddit, Spotify, CNN and dozens more websites in what authorities called the biggest cyberattack in the history of the internet.

Brian Krebs, a former Washington Post reporter who runs the influential cyber security blog KrebsonSecurity, said in January he was able to link Jha to the original code. Krebs also said his investigation linked the student to a series of cyber attacks on Rutgers' websites that began during the 2014-2015 school year.

At the time, Jha's father said the idea his son created something that could have crashed much of the internet from their house in Fanwood was ridiculous.

"I know what he is capable of," Anand Jha told NJ Advance Media in January. "Nothing of the sort of what has been described here has happened."

Jha said nothing as he left court in Trenton Wednesday.

"With support from his family, he'll get through this," said Stahl, his attorney.

Kelly Heyboer may be reached at kheyboer@njadvancemedia.com. Follow her on Twitter @KellyHeyboer. Find her at KellyHeyboerReporter on Facebook.

Ted Sherman may be reached at tsherman@njadvancemedia.com. Follow him on Twitter @TedShermanSL. Facebook: @TedSherman.reporter. Find NJ.com on Facebook.