Source:
https://www.reuters.com/article/us-usa-cyber/three-u-s-men-plead-guilty-to-crimes-tied-to-2016-botnet-attacks-idUSKBN1E71ZB

REUTERS

#CYBER RISK

DECEMBER 13, 2017 / 9:36 AM / 6 DAYS AGO

Three U.S. men plead guilty to crimes tied to 2016 botnet attacks

Dustin Volz, Nate Raymond

(Reuters) - A former Rutgers University student and two other men pleaded guilty to computer crimes related to the creation, sale and use of the Mirai botnet, a network of infected electronics equipment used to knock major websites offline in massive 2016 cyber attacks.

Rutgers University student Paras Jha is seen as he leaves the Clarkson S. Fisher Building and U.S. Courthouse after his hearing in Trenton, New Jersey, U.S., December 13, 2017. REUTERS/Dominick Reuter

Paras Jha, 21, pleaded guilty in federal court on Friday to charges involving writing code that allowed him to infect and control devices with Mirai, the Justice Department said on Tuesday.

He also pleaded guilty on Wednesday in federal court in New Jersey to hacking that repeatedly shut down the Rutgers University computer system between 2014 and 2016, paralyzing the school's networks for days at a time.

Two other individuals, Josiah White, 20, and Dalton Norman, 21, also pleaded guilty to charges related to the development and use of Mirai for criminal gain. Jha and Norman also pleaded guilty to a separate online advertising fraud scheme.

The Mirai botnet was used to infect hundreds of thousands of internet-connected devices including webcams, which its creators then turned into bots that attacked websites and internet infrastructure in "denial of service" assaults that knocked them offline.

Those attacks included one in October 2016 on an internet infrastructure firm known as Dyn that disrupted access to dozens of websites across the United States and Europe including ones run by Twitter Inc, PayPal Holdings Inc and Spotify. Authorities said Jha and his accomplices did not carry out that specific attack, which took place after an individual believed to be Jha published Mirai's source code online.

U.S. Acting Deputy Assistant Attorney General Richard Downing declined to comment when asked during a press call about the status of identifying those responsible for the Dyn attack.

Jha began to create the Mirai botnet in August 2016 to launch powerful denial of service attacks targeting business competitors and others against whom the attackers "held grudges," prosecutors said in court documents. He owned a service denial mitigation company called ProTraf Solutions, according to his LinkedIn page.

Jha and his co-conspirators also sought financial gain, renting the botnet out to other criminals. Jha attempted to destroy or conceal evidence of his crimes by erasing the virtual machine used to run Mirai and posting the code online to create "plausible deniability," prosecutors said.

In August 2016, White created the scanner that was part of the Mirai code, which helped the botnet identify devices that could be accessed and infected, charging documents said.

The exterior of the Clarkson S. Fisher Building and U.S. Courthouse, where Rutgers University student Paras Jha had a hearing, is seen in Trenton, New Jersey, U.S., December 13, 2017. REUTERS/Dominick Reuter

In September 2016, Norman and accomplices expanded Mirai, allowing it to infect more than 300,000 devices, prosecutors said. Court documents did not accuse Norman of creating Mirai but said he helped monetize its use.

In a separate case unsealed on Tuesday, Jha and Norman were charged with leveraging another botnet for a different scheme to generate online ad revenue through fraudulent clicks, a practice known as clickfraud.

Jha admitted to earning about 200 bitcoin, which was valued at $180,000 on Jan. 29, as a result of the clickfraud, prosecutors said. The amount would be worth about $3.4 million today.

Former Rutgers University student Paras Jha had a hearing, is seen as he leaves the Clarkson S Fisher Building and U.S. Courthouse after his hearing in Trenton, New Jersey, U.S., December 13, 2017. REUTERS/Dominick Reuter

Robert Stahl, Jha's attorney, said his client had been released pending sentencing and has not been a student at New Jersey's Rutgers University since December 2016.

"Starting when he was just 19 years old, (Jha) made a series of mistakes with significant consequences that he only now fully appreciates," Stahl said in a statement. "He is extremely remorseful and accepts full responsibility for his actions."

Attorneys for White and Norman did not respond to requests for comment.

Jha's name surfaced in January, when the cyber website Krebs On Security reported he may have been behind the online persona Anna-Senpai, who claimed to be the author of the Mirai worm.

Anna-Senpai released the source code of the Mirai botnet online in September 2016, which gave other hackers the opportunity to use it. A month later the massive assault on infrastructure firm Dyn took place, causing swaths of the internet to be temporarily unavailable.

In court on Wednesday, Jha acknowledged his hacks caused Rutgers to lose $3.5 million to $9.5 million, Acting U.S. Attorney William Fitzpatrick told reporters.

In a statement, Rutgers said no data was compromised and that it had made “substantial improvements” to its technology infrastructure.

Reporting by Dustin Volz in Washington, Nate Raymond in Boston and Jim Finkle in Toronto; editing by Richard Chang and Cynthia Osterman

Our Standards: *The Thomson Reuters Trust Principles.*