Source:
https://www.law360.com/whitecollar/articles/994291/3-men-cop-to-mirai-malware-attacks-in-nj-alaska

3 Men Cop To Mirai Malware Attacks In NJ, Alaska

By **Jeannie O'Sullivan**

Law360, New York (December 13, 2017, 8:42 PM EST) -- Three men have copped to cyberattacks in New Jersey and Alaska involving the malicious software known as Mirai that paralyzed computer systems, including at Rutgers University, and temporarily blocked access to popular websites such as Twitter, Netflix and Amazon, in what federal prosecutors described Wednesday as one of their largest criminal malware takedowns to date.

In October 2016, more than 100,000 computers were **impacted by botnets**, or collections of computers controlled by malware unbeknownst to their owners, operated by Paras Jha, 21, of Fanwood, New Jersey; Dalton Norman, 21, of Metairie, Louisiana; and Josiah White, 20, of Washington, Pennsylvania, U.S. Department of Justice officials announced Wednesday along with federal prosecutors in New Jersey and Alaska. The defendants pled guilty this month to conspiracy to violate the federal Computer Fraud and Abuse Act and face possible prison time.

The trio met online and wrote the source code for a botnet that conducted “distributed denial of service,” or DDoS, attacks that effectively shut down servers, while Norman and Jha also orchestrated a “click-fraud" scheme used to generate phony advertising revenue, and Jha launched separate attacks on servers at Rutgers, where he was previously a student. They reaped profits by renting the botnets out to other hackers and extorting hosting providers into paying protection money to prevent the DDoS attacks, prosecutors said.

All three suspects pled guilty Dec. 8 to criminal charges in the District of Alaska, where the first attacks occurred, stemming from their operation of the Mirai botnet, which carried out the DDoS attacks in devices such as wireless cameras, routers and digital video recorders. Jha and Norman additionally copped to operating the click-fraud botnet, which affected

mostly home-based internet routers.

On Wednesday, Jha also tendered a guilty plea in the District of New Jersey to executing a series of attacks on the networks of Rutgers University.

“As more and more of our everyday devices become connected to the internet this case brings to light how significant some of these threats against us are,” acting Deputy Assistant Attorney General Richard W. Downing of the Criminal Division told reporters during a conference call.

Jha’s attorneys, Robert Stahl and Laura K. Gasiorowski of the Law Offices of Robert G. Stahl, said in a statement that their client was remorseful and accepts full responsibility for his actions.

“Paras Jha is a brilliant young man whose intellect and technical skills far exceeded his emotional maturity,” the statement said.

An attorney for Norman didn’t immediately respond to a requests for comment, and Law360 was unsuccessful in reaching White’s public defender.

The Mirai botnet utilized vulnerabilities in victims’ devices that allowed the defendants to gain control over them, according to prosecutors. The defendants used it from the summer of 2016 to the fall of that year, when Jha posted its source code on a criminal forum. Other hackers have since used Mirai variants to launch their attacks, prosecutors said.

Jha and Norman operated the click-fraud botnet from December 2016 to February 2017, targeting primarily U.S.-based computing devices such as home internet routers, prosecutors said. The scheme makes it appear that a real user has “clicked” on an advertisement for the purpose of artificially generating revenue.

The Rutgers attacks were carried out between November 2014 and September 2016 and disrupted the university’s central authentication server, which facilitated communications among staff, faculty and students regarding assignments and assessments, prosecutors said.

The attacks coincided with midterms, finals and class registration times, according to

William Fitzpatrick, acting U.S. Attorney for the district of New Jersey. The scheme "effectively paralyzed the system for days at a time," he said.

Asked by reporters about Jha's possible motive, Fitzpatrick said anger at the school or the desire to "show off" could be "reasonable inferences."

The Mirai botnet and click-fraud botnet cases are being prosecuted by Assistant U.S. Attorneys Adam Alexander and C. Alden Pelker. The Rutgers University case is being prosecuted by Assistant U.S. Attorney Shana Chen.

Jha is represented by Robert G. Stahl and Laura K. Gasiorowski of the Law Offices of Robert G. Stahl.

Norman is represented by David A. Nesbett of Nesbett & Nesbett PC.

White is represented by federal public defender Richard Curtner.

The Mirai cases are U.S. v. Jha, case no. 3:17-cr-00164, U.S. v. Norman, case no. 3:17-cr-00167, and U.S. v. White, case no. 3:17-cr-00165, in the U.S. District Court for the District of Alaska.

The click-fraud cases are U.S. v. Jha, case no. 3:17-cr-00163, and U.S. v. Norman, case no. 3:17-cr-00166, in the U.S. District Court for the District of Alaska.

The Rutgers case is U.S. v. Jha, in the U.S. District Court for the District of New Jersey. The case number was unavailable Wednesday.