

Three plead guilty in Mirai botnet attacks

December 13 2017

US officials unveiled criminal charges Wednesday against a former university student and two others in the Mirai botnet attacks which shut down parts of the internet in several countries starting in mid-2016.

The Justice Department announced plea agreements for Paras Jha, 21—a former Rutgers University computer science student who acknowledged writing the malware code—and Josiah White, 20, and Dalton Norman, 21, who helped profit from the [attacks](#).

In documents unsealed Wednesday, Jha admitted writing the code for the botnet which harnessed more than 100,000 "internet of things" (IoT) devices such as cameras, light bulbs and appliances to launch the attacks.

By commanding an army of bots—or computers under control of the attackers—the malware shut down networks and websites in the United States, Germany, Liberia and elsewhere.

Jha admitted he "set up and managed command and control servers to manage the infected computers" in the scheme.

Officials said the three used the botnet "to conduct a number of powerful distributed denial-of-service" attacks which flood the internet and can shut down networks.

Later, Jha posted the source code for the Mirai malware on a criminal forum, allowing other groups to use it.

The malware was used to make money through "click fraud," a scheme that makes it appear that a real user has clicked on an advertisement for the purpose of artificially generating revenue, according to [officials](#).

The three generated some \$180,000 from the scheme in bitcoin, Justice officials added.

Jha was identified as a suspect earlier this year by security blogger Brian Krebs—who was himself a victim of the attacks.

Krebs said Jha used the online moniker Anna-Senpai, who had claimed responsibility for earlier denial of service attacks using various versions of Mirai—including some targeting Rutgers University, the school in New Jersey where Jha was studying.

In January 2017, "Jha and his co-conspirators leased access to their botnet to other criminals in exchange for payment," according to the plea agreement in federal court.

According to Krebs, Jha and White operated ProTraf Solutions LLC, which masqueraded as a security firm that dealt with "denial of service" attacks it created.

The three face possible prison terms and monetary fines as a result of the conspiracy and fraud charges.

Jha pleaded guilty separately to a series of attacks which shut down the Rutgers computer networks from 2014 to 2016, officials said.

© 2017 AFP

Citation: Three plead guilty in Mirai botnet attacks (2017, December 13) retrieved 27 April 2024 from <https://phys.org/news/2017-12-guilty-mirai-botnet.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.