Source:
http://www.zdnet.com/article/justice-dept-indicts-mirai-botnet-attackers/

Mirai botnet attackers plead guilty for roles in cyberattacks

The Mirai botnet threw vast swathes of the US internet offline in a cyberattack last year.

By Zack Whittaker for Zero Day | December 13, 2017 -- 14:43 GMT (06:43 PST) | Topic: Security

(Image: file photo)

Three men have pleaded guilty to federal cyber-crime charges for launching a cyberattack last year that knocked large parts of the internet offline.

Paras Jha, Josiah White, and Dalton Norman were indicted by an Alaska court in early December, according to documents unsealed Wednesday.

The Justice Dept. released a statement later in the day confirming the news (https://www.justice.gov/opa/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases-involving).

Prosecutors accused the hackers of writing and using the Mirai botnet to hijack vulnerable internet-connected devices to launch powerful distributed denial-of-service (DDoS) attacks.

According to Jha's plea agreement (https://www.documentcloud.org/documents/4327736-Paras-Jha-plea-agreement.html), the botnet ensnared more than 300,000 vulnerable devices.

The filing says that Jha "conspired to conduct DDoS attacks against websites and web hosting companies located in the United States and abroad," and "demanded payment in exchange for halting the attack."

DDoS attacks are a common way to disrupt online services, and often require little or no technical knowledge. The operator uses ensnared, vulnerable devices to flood a domain or server with bandwidth, which in turn can prevent legitimate access from accessing sites and services.

Jha admitted to releasing the code publicly to create "plausible deniability" if code was found on his computers. The publishing of that code effectively made the botnet open source, so that anyone can use (http://www.zdnet.com/article/source-code-of-mirai-botnet-responsible-for-krebs-on-security-ddos-released-online/) the botnet to launch attacks.

White pleaded guilty (https://www.documentcloud.org/documents/4327763-Josiah-White-plea-agreement.html) to creating the Mirai botnet's scanner, used to seek out and hijack vulnerable internet-connected devices. Norman admitted (https://www.documentcloud.org/documents/4327975-Dalton-Norman-plea-agreement.html) to developing exploits to build into the botnet.

Contact me securely (https://medium.com/@zackwhittaker/how-to-contact-me-securely-38dc5c5bc756)

Zack Whittaker can be reached securely on Signal and WhatsApp at 646-755–8849, and his PGP fingerprint for email is: 4D0E 92F2 E36A EC51 DAAE 5D97 CB8C 15FA EB6C EEA5.

Read More (https://medium.com/@zackwhittaker/how-to-contact-me-securely-38dc5c5bc756)