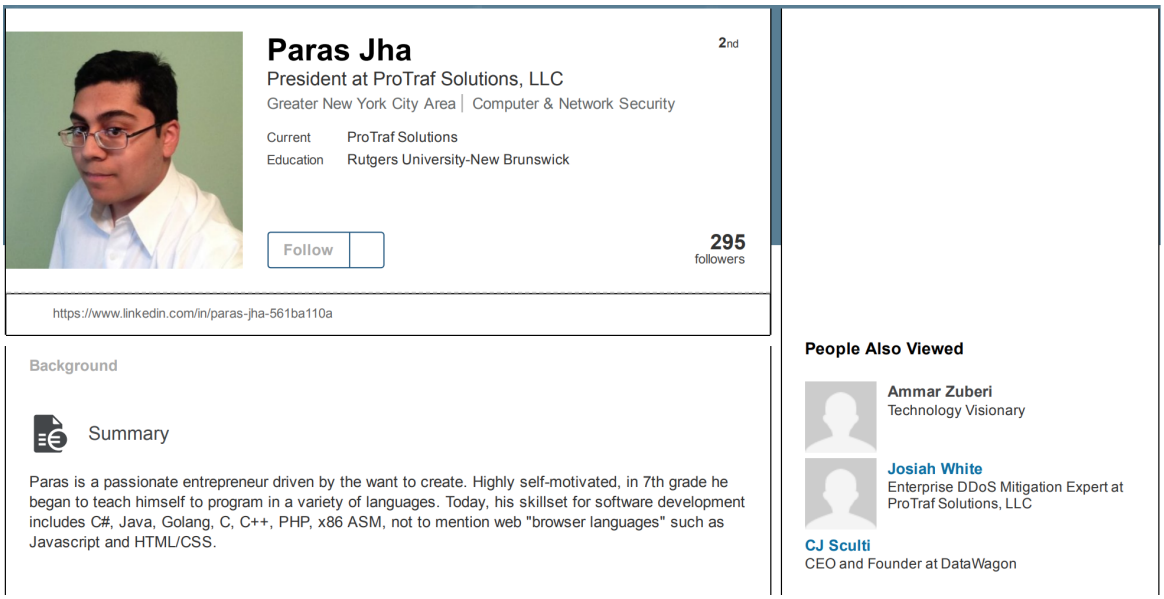
Mirai IoT Botnet Co-Authors Plead Guilty

krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/

The **U.S. Justice Department** on Tuesday unsealed the guilty pleas of two men first identified in January 2017 by KrebsOnSecurity as the likely co-authors of **Mirai**, a malware strain that remotely enslaves so-called “Internet of Things” devices such as security cameras, routers, and digital video recorders for use in large scale attacks designed to knock Web sites and entire networks offline (including multiple major attacks against this site).

Entering guilty pleas for their roles in developing and using Mirai are 21-year-old **Paras Jha** from Fanwood, N.J. and **Josiah White**, 20, from Washington, Pennsylvania.



Jha and White were co-founders of **Protraf Solutions LLC**, a company that specialized in mitigating large-scale DDoS attacks. Like firemen getting paid to put out the fires they started, Jha and White would target organizations with DDoS attacks and then either extort them for money to call off the attacks, or try to sell those companies services they claimed could uniquely help fend off the attacks.

CLICK FRAUD BOTNET

In addition, the Mirai co-creators pleaded guilty to charges of using their botnet to conduct click fraud — a form of online advertising fraud that will cost Internet advertisers more than $16 billion this year, according to estimates from ad verification company **Adloox.**

The plea agreements state that Jha, White and another person who also pleaded guilty to click fraud conspiracy charges — a 21-year-old from Metairie, Louisiana named **Dalton Norman** — leased access to their botnet for the purposes of earning fraudulent advertising

revenue through click fraud activity and renting out their botnet to other cybercriminals.

As part of this scheme, victim devices were used to transmit high volumes of requests to view web addresses associated with affiliate advertising content. Because the victim activity resembled legitimate views of these websites, the activity generated fraudulent profits through the sites hosting the advertising content, at the expense of online advertising companies.

Jha and his co-conspirators admitted receiving as part of the click fraud scheme approximately two hundred bitcoin, valued on January 29, 2017 at over $180,000.

Prosecutors say Norman personally earned over 30 bitcoin, valued on January 29, 2017 at approximately $27,000. The documents show that Norman helped Jha and White discover new, previously unknown vulnerabilities in IoT devices that could be used to beef up their Mirai botnet, which at its height grew to more than 300,000 hacked devices.

MASSIVE ATTACKS

The Mirai malware is responsible for coordinating some of the largest and most disruptive online attacks the Internet has ever witnessed. The biggest and first to gain widespread media attention began on Sept. 20, 2016, when KrebsOnSecurity came under a sustained distributed denial-of-service attack from more than 175,000 IoT devices (the size estimates come from this Usenix paper (PDF) on the Mirai botnet evolution).

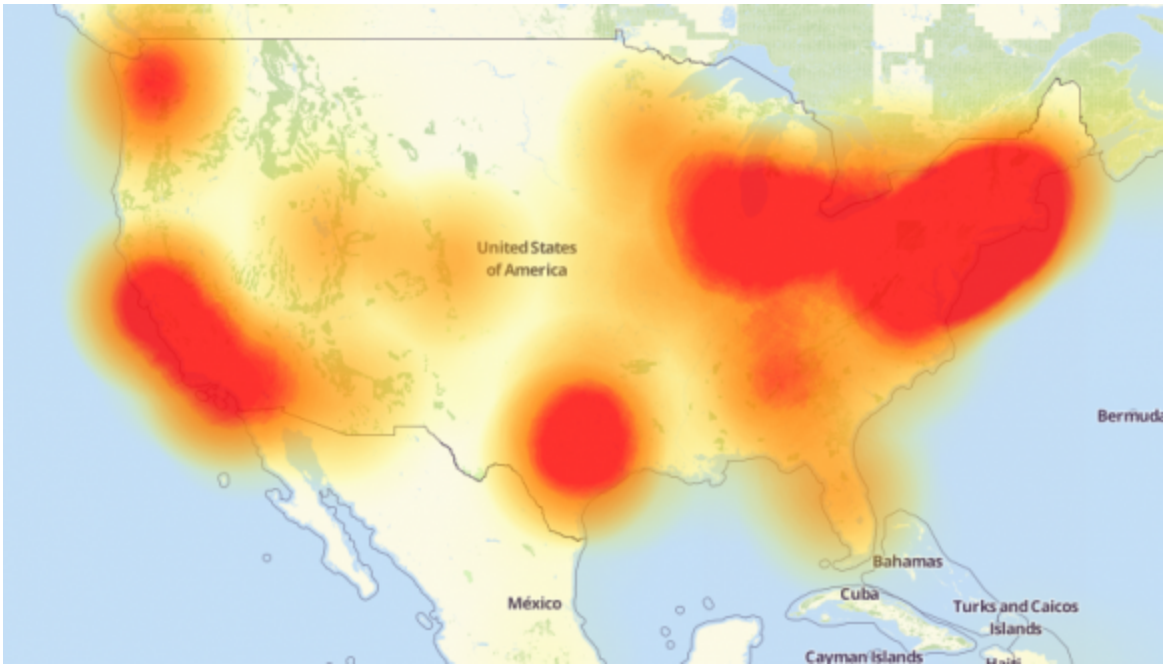
That September 2016 digital siege maxed out at 620 Gbps, almost twice the size of the next-largest attack that **Akamai** — my DDoS mitigation provider at the time — had ever seen.

The attack continued for several days, prompting Akamai to force my site off of their network (they were providing the service pro bono, and the attack was starting to cause real problems for their paying customers). For several frustrating days this Web site went dark, until it was brought under the auspices of Google's Project Shield, a program that protects journalists, dissidents and others who might face withering DDoS attacks and other forms of digital censorship because of their publications.

At the end of September 2016, just days after the attack on this site, the authors of Mirai — who collectively used the nickname "Anna Senpai" — released the source code for their botnet. Within days of its release there were multiple Mirai botnets all competing for the same pool of vulnerable IoT devices.

The Hackforums post that includes links to the Mirai source code.

Some of those Mirai botnets grew quite large and were used to launch hugely damaging attacks, including the Oct. 21, 2016 assault against Internet infrastructure firm Dyn that disrupted **Twitter**, **Netflix**, **Reddit** and a host of other sites for much of that day.



A depiction of the outages caused by the Mirai attacks on Dyn, an Internet infrastructure company. Source: Downdetector.com.

The leak of the Mirai source code led to the creation of dozens of copycat Mirai botnets, all of which were competing to commandeer the same finite number of vulnerable IoT devices. One particularly disruptive Mirai variant was used in extortion attacks against a number of banks and Internet service providers in the United Kingdom and Germany.

In July 2017, KrebsOnSecurity published a story following digital clues that pointed to a U.K. man named **Daniel Kaye** as the apparent perpetrator of those Mirai attacks. Kaye, who went by the hacker nickname “Bestbuy,” was found guilty in Germany of launching failed Mirai

attacks that nevertheless knocked out Internet service for almost a million Deutsche Telekom customers, for which he was given a suspended sentence. Kaye is now on trial in the U.K. for allegedly extorting banks in exchange for calling off targeted DDoS attacks against them.

Not long after the Mirai source code was leaked, I began scouring cybercrime forums and interviewing people to see if there were any clues that might point to the real-life identities of Mirai's creators.

On Jan 18, 2017, KrebsOnSecurity published the results of that four-month inquiry, Who is Anna Senpai, the Mirai Worm Author? The story is easily the longest in this site's history, and it cited a bounty of clues pointing back to Jha and White — two of the men whose guilty pleas were announced today.

A tweet from the founder and CTO of French hosting firm OVH, stating the intended target of the Sept. 2016 Mirai DDoS on his company.

According to my reporting, Jha and White primarily used their botnet to target online gaming servers — particularly those tied to the hugely popular game **Minecraft**. Around the same time as the attack on my site, French hosting provider OVH was hit with a much larger attack from the same Mirai botnet (see image above), and the CTO of OVH confirmed that the target of that attack was a Minecraft server hosted on his company's network.

My January 2017 investigation also cited evidence and quotes from associates of Jha who said they suspected he was responsible for a series of DDoS attacks against **Rutgers University**:During the same year that Jha began studying at the university for a bachelor's degree in computer science, the school's servers came under repeated, massive attacks from Mirai.

With each DDoS against Rutgers, the attacker — using the nicknames "og_richard_stallman," "**exfocus**" and "**ogexfocus**," — would taunt the university in online posts and media interviews, encouraging the school to spend the money to purchase some kind of DDoS mitigation service.

It remains unclear if Jha (and possibly others) may face separate charges in New Jersey related to his apparent Mirai attacks on Rutgers. According to a sparsely-detailed press release issued Tuesday afternoon, the Justice Department is slated to hold a media conference at 2 p.m. today with officials from Alaska (where these cases originate) to "discuss significant cybercrime cases."

Update: 11:43 a.m. ET: *The New Jersey Star Ledger* just published a story confirming that Jha also has pleaded guilty to the Rutgers DDoS attacks, as part of a separate case lodged by prosecutors in New Jersey.

PAYBACK

Under the terms of his guilty plea in the click fraud conspiracy, Jha agreed to give up 13 bitcoin, which at current market value of bitcoin (~$17,000 apiece) is nearly USD $225,000.

Jha will also waive all rights to appeal the conviction and whatever sentence gets imposed as a result of the plea. For the click fraud conspiracy charges, Jha, White and Norman each face up to five years in prison and a $250,000 fine.

In connection with their roles in creating and ultimately unleashing the Mirai botnet code, Jha and White each pleaded guilty to one count of conspiracy to violate 18 U.S.C. 1030(a)(5)(A). That is, to "causing intentional damage to a protected computer, to knowingly causing the transmission of a program, code, or command to a computer with the intention of impairing without authorization the integrity or availability of data, a program, system, or information."

For the conspiracy charges related to their authorship and use of Mirai, Jha and White likewise face up to five years in prison, a $250,000 fine, and three years of supervised release.

This is a developing story. Check back later in the day for updates from the DOJ press conference, and later in the week for a follow-up piece on some of the lesser-known details of these investigations.

The Justice Department unsealed the documents related to these cases late in the day on Tuesday. Here they are:

Jha click fraud complaint (PDF)
Jha click fraud plea (PDF)
Jha DDoS/Mirai complaint (PDF)
Jha DDoS/Mirai plea (PDF)

White DDoS complaint (PDF)
White DDoS/Mirai Plea (PDF)
Norman click fraud complaint (PDF)
Norman click fraud plea (PDF)