**Anna Senpai**

Anna\_Senpai//Paras Jha//jorgemichaels //ogmemes123123//lelddos (member)//dreadiscool

**Criminal History:**

* Extortion
* Racketeering
* DDoS-for-hire
* IoT Botnet Mirai Author

**Anna Senpai, or Paras Jha, is a DDoS extortionist that gained his “fame” by authoring the majority of the Mirai botnet, while running a DDoS mitigation firm with a very checkered past. Brian Krebs deserves the credit for this portion of the project, as much of my research so far has been based off of his report on the Mirai author’s identity. It truly was an incredible read, one that read like a spy novel detailing one of history’s strangest tales of extortion.**

**One of HackForum’s “claims to fame” was the publishing of the Mirai source code on the forum in October 2016 by a user named Anna\_Senpai. The user on the forum had been posting for a few months bragging about taking down bots belonging to the Qbot botnet. The user said they had used their own botnet to detect and eradicate bots on their own botnet. After the Mirai dump, attacks using the botnet increased, but even before, the botnet was being used at an alarming scale.**

**Mirai was being used to extort owners of Minecraft servers and the mitigation companies that claimed to protect them. At the same time, unbeknownst to the victims at first but becoming more and more apparent, the Mirai botmaster was running a shady mitigation firm of their own, a company named ProTraf.**

**ProTraf employed technicians who had an admitted history of server takeover. Ammar Zuberi admitted he had taken over the address space of his former business FastReturn and turned it over to ProTraf. Brian Krebs implicated ProTraf and several other mitigation companies in unethical and potentially illegal mitigation techniques that involved transferring control of the address space to the mitigation company in order to deflect the attack.**

**Anna Senpai’s ultimate downfall was his knack for extortion and bragging. He targeted bigger names in the mitigation industry, as well as Brian Krebs, a well known cyber security analyst and seemingly a human honeypot for Hack Forums users and other annoying script kiddies. He bragged to Robert Coelho, one of his victims and owner of ProxyPipe, a DDoS mitigation firm, as well as Brian Krebs himself. This, coupled with long-forgotten vanity sites, social media sites, and conversations with former coworkers, lead to the completion of Brian Krebs’s investigation.**

**In the end, by connecting Anna Senpai to other monickers used in similar DDoS extortion attacks, the author of the Mirai botnet ended up being Paras Jha, an employee of ProTraf and a braggart. His relationship with Ammar Zuberi lead him to brag about his DDoS campaign, and Ammar went to Brian. Jha denies it all, including allegations that the FBI was investigating his DDoS campaigns.**

**Targets:**

**Minecraft Servers (DDoS and extortion)**

**DDoS mitigation firms (DDoS and extortion)**

**Rutgers University (DDoS)**

**Connections:**

**ProTraf Solutions**

**Lelddos**

**Money Crew**

**Amaar Zedib**

**Christopher “CJ” Sculti, Jr.**

**Josiah White // Litespeed**

**Vyp0r**

**Nightmare Group**