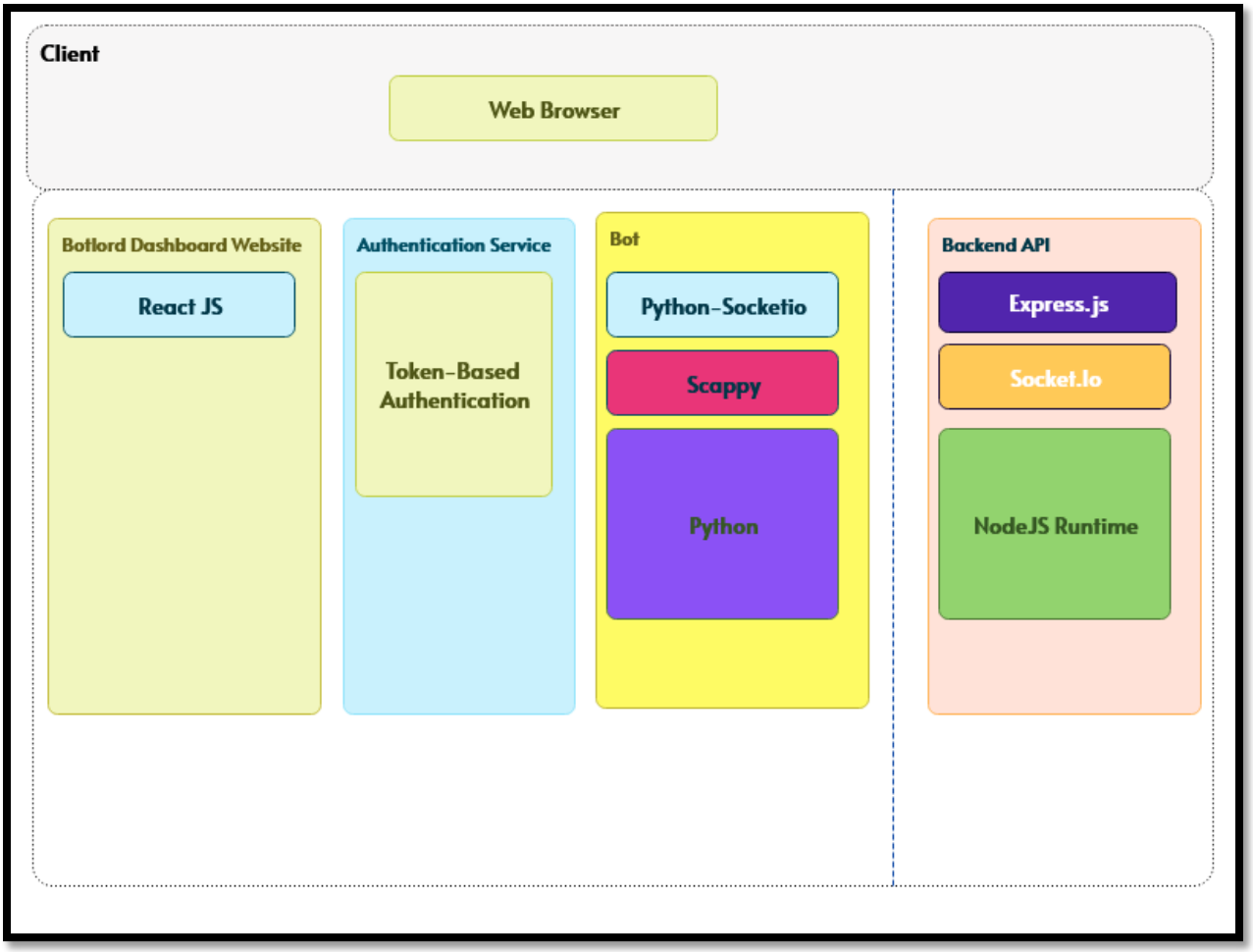
(D)DoS Project

How does it all work

System architecture



Component details

Botlord backend

The Botlord is a socket.io/express server that controls all the bots under it. It commands the bots to send DoS attacks to a certain IP address and port. Client server model is used to control the bots.

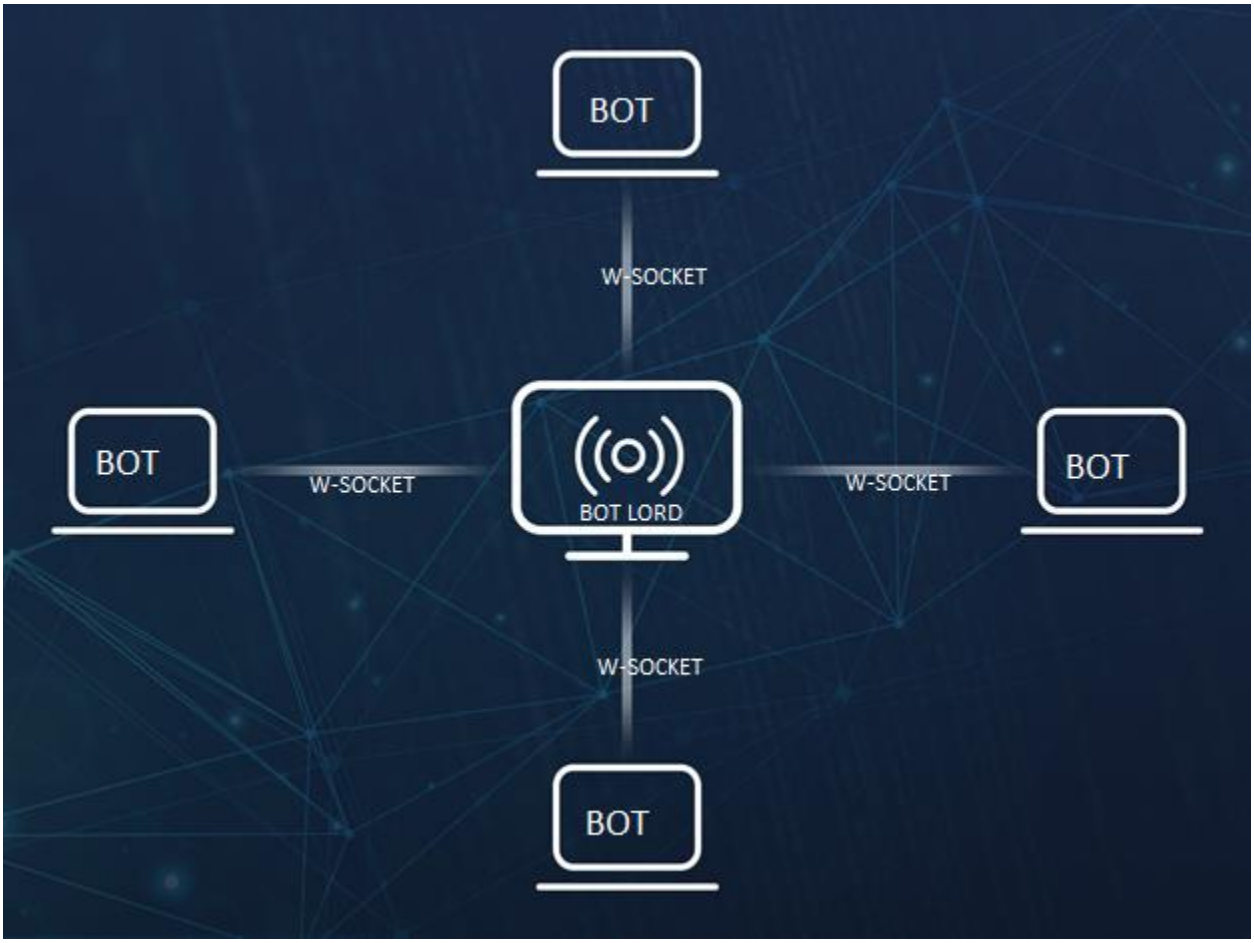
Bots

The Bots are python programs on infected pcs with socket clients that are connected to the botlord then await requests to perform DDoS attacks.

How do we deploy the malware onto target pcs?

We'll use a trojan horse program to deploy the malware. The malware will be hidden in a custom installer we made for "Telegram" app that installs Telegram and also installs the malware on the target system, then add it to startup programs so it gets initialized every time the system starts.

Bots' connection to the botnet



Zombie lord dashboard

The Dashboard connects to the server then the attacker can perform 3 types of DDoS attacks with the botnet ICMP flood, SYN flood and UDP flood. The attacker can also see the status of the botnet with some details on the dashboard.