Abstract

Nowadays everything is connected to the internet including iot devices like cameras, smart tv, etc. Like this almost anything can be connected to the internet and access from anywhere from the world. And we have seen these advantages have been misused by cyber criminals. They started making unsecured devices become a part of their botnets, infecting and spreading crytominers and randsomewares over the networks. Also they remotely access our devices to compromise bank accounts, private datas, etc. Even though we install AVs in our computers and mobile devices other devices are still exposed to attacks. In Order to get protected from these we are developing a security device called NIDDS (Network Intrusion Detection and Deduce System). This will be connected in between end devices and the internet and all tracks of malicious and suspicious traffic will be tracked and monitored. As we know AVs use signature based detections and can be evaded, our device will use an online malware detection system (Virus Total) and open source dynamic black lists which contain malware or suspicious programs along with some static pre compiled blacklists from different antivirus providers and our own definitions of block to filter the traffic to produce detailed log reports.

Architecture