# Mirai Dyn DDoS Attack

## Attack Principle

In October 2016 a major Domain name service provider was attacked. The attack was generated by the Mirai software. This was a multi-vectored that used tens of millions IP addresses to carry out the attack. It achieved 1 terabit per second traffic. It achieves this by infecting compromised IoT devices. It does this by searching the internet for IoT devices that still use their default passwords. The attacker then uses command and control center to sends SYN and TCP/UDP packets as well as application layer attacks to flood the victim with requests. This will cause the victim's server to crash.

## Consequences

This resulted in outages of many major web sites such as Reddit, Github, PayPal, etc. In addition to this, the Mirai source code is on the internet. It is now easier than ever to conduct DDoS attacks.

## Defenses

To mitigate an attack, you should disable any unused or insecure protocols. Such as Telnet or UPnP. This can make it harder to access unsecured IoT devices that could be used in an attack. In addition to this, you could monitor all incoming packets for suspicious activity. You could also setup blacklists/whitelists to control access.