Slow Loris Denial-of-Service Attack

How does it work?
Slow Loris works by opening many connections to a target server and sending partial HTTP requests. It keeps these connections open for as long as possible by sending tiny bits of data at regular intervals, preventing the server from closing the connections and allocating resources to legitimate traffic.

Why is it unique compared with other high-bandwidth DDoS attacks?
This is different from traditional DDoS, that would depend on saturating a server with a huge amount of traffic; Slow Loris uses only a minimal amount. It depends on consuming connection resources through slow and incomplete requests, which usually are difficult to detect and mitigate by bandwidth-based solutions.

What does this attack do?
Slow Loris forces the affected web server to waste all its resources on handling the attack, thus not being able to respond to other legitimate client requests. This will create unavailability of the service without requiring overwhelming volumes of traffic.

How can you mitigate/prevent the effects of the attack?

For mitigation techniques, one can provide:

Limit the number of connections from the same source IP address.
Setting timeouts to incomplete HTTP headers
Application firewalls and load balancers or reverse proxies- distribution of connections.
Employing special modules, such as mod_antiloris for Apache, which can block Slow Loris attacks.

Are there any more high-profile results of this attack being conducted?
Among several other incidents, Slow Loris was employed during the mass protests following the 2009 Iranian presidential election to take down Iranian government sites. Its low-bandwidth nature made it well-suited to activists with limited resources.

Sources :

1 . https://www.imperva.com/learn/application-security/slowloris/

2. https://www.radware.com/security/ddos-knowledge-center/ddospedia/slowloris