The world's largest DDoS attack took GitHub offline for fewer than 10 minutes

Jon Russell @jonrussell / Mar 2, 2018

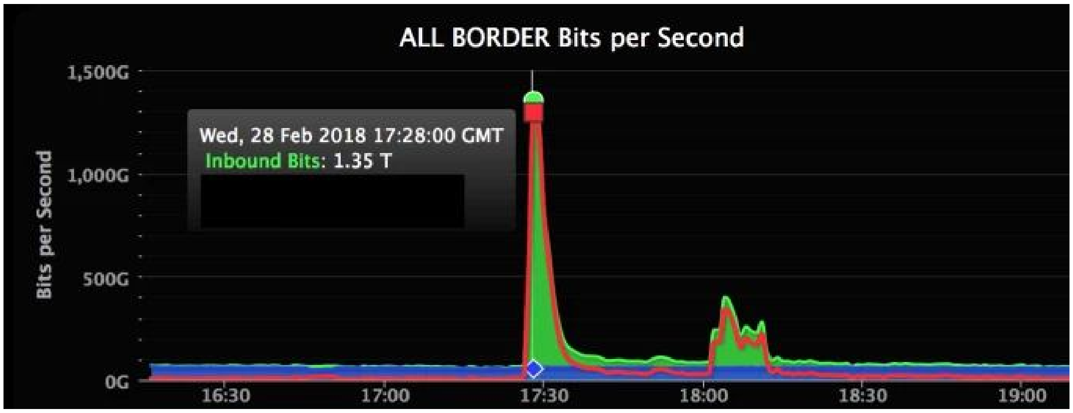
In a growing sign of the increased sophistication of both cyber attacks and defenses, **GitHub** has revealed that this week it weathered the largest-known DDoS attack in history.

DDoS — or distributed denial of service in full — is a cyber attack that aims to bring websites and web-based services down by bombarding them with so much traffic that their services and infrastructure are unable to handle it all. It's a fairly common tactic used to force targets offline.

GitHub is a common target — the Chinese government was widely suspected to be behind a five-day-long attack in 2015 — and this newest assault tipped the scales at an incredible 1.35Tbps at peak.

In a blog post retelling the incident, GitHub said the attackers hijacked something called “memcaching” — a distributed memory system known for high-performance and demand — to massively amplify the traffic volumes that were being fired at GitHub. To do that, they initially spoofed GitHub’s IP address and took control of memcached instances that GitHub said are “inadvertently accessible on the public internet.”

The result was a huge influx of traffic. Wired reports that, in this instance the memcached systems used amplified the data volumes by around 50 times.



GitHub’s inbound traffic skyrocketed during the attack

GitHub called in assistance from Akamai Prolexic, which rerouted traffic to GitHub through its “scrubbing” centers, which removed and blocked data deemed to be malicious. Following eight minutes of the assault, the attackers called it off and the DDoS stopped.

In total, GitHub was offline for five minutes between 17:21 to 17:26 UTC, with intermittent connectivity between 17:26 to 17:30 UTC.

The service has become critical for any company handling code — very many, indeed — so while an outage is never welcomed, the response in this case is impressive and certainly bodes well. GitHub said it continues to analyze this attack, and others, to ensure it is suitably defended.

You can read full details in this GitHub blog post.