Microsoft says June Outlook outages were a DDoS attack

In early June, complaints began cropping up on Twitter that Outlook was down for as many as 18,000 users at the peak of what, it turns out, was a Distributed Denial-of-Service (DDoS) attack, according to a story in *The Associated Press* (*AP*) this morning. Microsoft acknowledged the attack in a blog post on Friday, offering some technical details and recommendations for guarding against such attacks in the future.

The *AP* article said a spokeswoman (presumably for Microsoft, though it's not explicitly clear in the article) confirmed the group to be Anonymous Sudan, a group that has been active since at least January, says an article in *Cybernews*, which reported on the attack the day it happened. Per that article, the group claimed its attack lasted about an hour and a half before it stopped.

According to a former National Security Agency offensive hacker named Jake Williams quoted in the *AP* story, there is "no way to measure the impact if Microsoft doesn't provide that info," and he wasn't aware of Outlook having been hit this hard before.

In 2021, Microsoft mitigated what was then one of the largest DDoS attacks ever recorded, which lasted more than 10 minutes with traffic peaking at 2.4 terabits per second (Tbps). In 2022, an attack reached 3.47Tbps. It's not clear how large traffic bursts were in the June attack.

The DDoS activity, Microsoft says in its blog post, targeted OSI layer 7 – that is, the layer of a network where applications access network services. It's where your apps,

like email, call out for their data. Microsoft believes the attackers, which it calls Storm-1359, used botnets and tools to launch its attacks “from multiple cloud services and open proxy infrastructures,” and that it appeared to be focused on disruption and publicity.

We’ve reached out to Microsoft for comment, and will update here if we receive a response.

https://www.theverge.com/2023/6/18/23765124/microsoft-outlook-june-ddos-attack-anonymous-sudan