Anatomy of a Failed DDoS Attack

What we know:

Lumen mitigated its largest attack to date: 1.06 Tbps

The customer experienced no downtime, so **the attacker failed.**

The target was a gaming service hosted by a Lumen DDoS Mitigation customer.

What we observed:

Three unique Command and Controls (C2s) issued attack orders on four different dates and times.

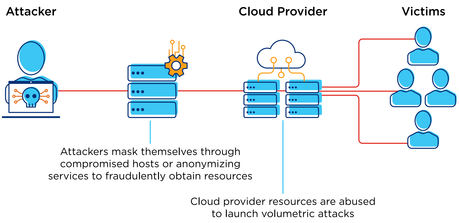
Threat actor tested several attack methods and probed the target's network defenses for several days.

Probing attacks utilized numerous attack vectors to bypass countermeasures, overhwelm the host, and launch application-specific attacks.

In their last effort to disrupt the intended victim, the threat actor tried (and failed) to launch a 1.06Tbps, UDP-based attack that resulted in a traffic spike roughly 20,000 times larger than normal.

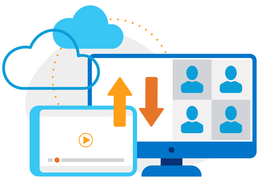
TREND TO WATCH: Threat actor leveraged cloud-based services in a fraudulent way to significantly boost attack capabilities.

What a cloud-services attack looks like:



What individual organizations can do to help stop these attacks:

1. If you're using a cloud service, ensure your accounts are protected by multifactor authentication. Account access and use should be routinely audited and follow good security practices.



2. Keep your services that are hosted in the cloud up to date (especially in terms of security patches) and monitor them for suspicious activity — like high usage rates.

3. If abuse is uncovered, take appropriate mitigative actions such as changing credentials, quarantining and cleaning impacted hosts, and removing or disabling any mechanisms that would allow the threat to persist within your cloud environment. In addition, consider alerting your cloud provider as the attack may have impacted multiple customers.

Read the full report →

LUMEN