Largest ever DDoS attack targeted AWS

Threat Memo - Date: 18/06/2020 - Version: 1.0
TLP:WHITE

FOR INFORMATION	Category	Type	Domain	Sector	Confidence
	Cybercrime	DDoS	World	Cloud services	A1

Key Points

- The largest DDoS attack ever recorded targeted AWS last February.
- The attack lasted three days and the traffic reached 2,3 Tbps.
- The attack highly likely targeted a single customer but had implications for the whole cloud services provider.

Summary

Various news sources reported[1] on June 17 that one of the biggest internet cloud services provider, Amazon Web Services (AWS) experienced in February 2020 what is probably the largest scale Distributed Denial of Service (DDoS) attack ever recorded. Amazon stated that measured traffic surges of up to 2,3 Tbps were successfully mitigated. Originally, information on the attack came from Amazon's AWS Shield, Threat Landscape Report for Q12020[2].

Additional details extracted from Amazon's report reveal that:

- The attack was highly likely not directed at the Amazon service itself but one of its customers (although not revealed who).
- The DDoS attack was implemented by using the reflection method on the LDAP alternative protocol CLDAP.
- The DDoS attack lasted about 3 days.
- The traffic surge was successfully handled using the defence mechanisms in place (Amazon's AWS shield).

The table below summarises some recent notable high-volume DDoS attacks.

Date	Reported by	Method	Peak traffic	Targeted organisation
Jun 2020	Arbor	Reflection attacks	1,44 Tbps	
Q1 2020	Link11[3]	Reflection attacks: DNS CLDAP, NTP, and WS-Discovery Use of public, cloud server-based botnets	406 Gbps	
Mar 2020	Cloudflare[4]		550 Gbps	
Feb 2020	Amazon	Reflection attack using CLDAP	2,33 Tbps	AWS
Mar 5, 2018	Arbor (Netscout)	Memcache server vulnerability reflection/amplification	1,7 Tbps	Customer of US based services provider
Feb 28, 2018	Akamai, Cloudflare, Arbor	Memcache server vulnerability reflection/amplification	1,7 Tbps	Github
Sep 21, 2016		Mirai botnet	665 Gbps	krebsonsecurity.com
Q3 2016	Arbor		650 Gbps	Site in Brazil

Comments

Currently, some EU institutions, bodies or agencies (EU-I) are users of AWS and could potentially have been affected by the DDoS attack.

Even though it has been successfully mitigated, the attack highlights a number of points to be considered in respect of cloud service usage:

[1] https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/
[2] https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf
[3] https://www.link11.com/en/blog/threat-landscape/q1-2020-link11-ddos-report-en/
[4] https://blog.cloudflare.com/network-layer-ddos-attack-trends-for-q1-2020/

- Even if a single cloud services customer is targeted, the DDoS attack can have implications on availability for all the service tenants.
- It is noteworthy that cyber actors have the capability to scale their attacks to traffic volumes previously unreachable which could impact even internet backbone lines.
- A big part of the internet continues to provide unsecured services which can be abused to generate DDoS traffic flows. As the Memcache experience has shown in the past, threat groups will for sure rush to use any new vulnerability as it becomes known.
- Although the victim and the motivation of the attack have not become known, an organisation may face the same situation for a number of reasons and should have developed a plan on how to handle similar situations in all stages of an attack.

CERT-EU will be releasing soon a general security guidance on threats to Cloud services.