Largest ever DDoS in PPS against a European bank

Threat Memo - Date: 03/07/2020 - Version: 1.0
TLP:WHITE

FOR INFORMATION	Category	Type	Domain	Sector	Confidence
	Cybercrime	DDoS	Europe	Banking	A1

Key Points

- The largest DDoS attack ever measured in packets per second (PPS) was mitigated by Akamai on June 21.
- The attack reached a peak of 809 million PPS, more than double the previous PPS record.
- The target was an unnamed European bank.

Summary

Public reporting[1] announced the largest Distributed Denial of Service (DDoS) attack ever, measured in packets per second (PPS), hit a European bank on June 21. At the peak, 809 million PPS hit the bank's systems. DDoS protection provider Akamai mitigated the attack that lasted less than 10 minutes. Network traffic levels rose from normal to peak level in a matter of seconds.

The source IP addresses for the attack were mostly (96.2 %) unseen in previous DDoS attacks, lending support to the hypothesis that a new botnet was used. The malicious packets contained only 1 data byte. Adding IP headers leads to a total packet size (including headers) of 29 bytes, a common and thus hard to detect packet size. This current attack broke the previous PPS record of 385 million PPS.

Several metrics can be used to compare DDoS attacks. Attacks with a high number of packets per second (PPS) are generally aimed at bringing down network devices or cloud apps. When a large number of bytes per second (BPS) is sent, attackers aim to exhaust the internet pipeline, and a large number of requests per second (RPS) attempts to bring down a webserver situated at the edge of an environment.

The Amazon Web Services DDoS attack of February 2020 was high in number of bytes per second. See also TM20-077. Table 1 shows a comparison between the current attack and the one against AWS last February.

Recent attack	Type	Victim	Volume in number of packets per second	Volume in bytes per second
June 21 2020	PPS	European bank	809M PPS	418 Gbps
February 2020	BPS	AWS client	293.1M PPS	2.3 Tbps

Table 1: Comparison between recent DDoS attacks.

Comments

The motivation behind the current attack is unknown. A plausible hypothesis could be that the authors wanted to test or demonstrate the capability of their new botnet.

Another possible motive could be a politically motivated disruptive attack. Indeed, entities in the financial sector have been usual targets for such kinds of operation. However, in such case, the attacks are usually preceded by announcements or come with claims for responsibility on social media, which was not apparently the case for this attack.

[1] https://www.bleepingcomputer.com/news/security/european-bank-suffers-biggest-pps-ddos-attack-new-botnet-suspected/