securityweek.com

Brian Krebs' Blog Hit by 665 Gbps DDoS Attack

Tags: NEWS & INDUSTRY Cybercrime

3-4 minutes

Investigative cybercrime journalist Brian Krebs reported on Tuesday that his website, KrebsOnSecurity.com, was hit by a massive distributed denial-of-service (DDoS) attack that could be the largest in history.

According to Krebs, his site was targeted with various types of DDoS attacks, including SYN and HTTP floods. The attack peaked at 665 Gbps and 143 Mpps (million packets per second), but it was successfully mitigated by Akamai, the company that provides DDoS protection services for KrebsOnSecurity.

> Holy moly. Prolexic reports my site was just hit with the largest DDOS the internet has ever seen. 665 Gbps. Site's still up. #FAIL
>
> — briankrebs (@briankrebs) September 21, 2016

Krebs believes that the botnet used to target his blog mostly consists of Internet of Things (IoT) devices, such as webcams and routers, that have default or weak credentials.

Akamai told Krebs that this attack was nearly twice the size of the largest attack they had previously encountered. It's worth noting

that [Arbor Networks reported](#) in January that some of its customers had been hit by attacks that peaked at 500, 450 and 425 Gbps.

In January, a group of anti-ISIS hackers claimed to have launched DDoS attacks on BBC websites that [peaked at 600 Gbps](#), but some experts [questioned their claims](#).

As for Brian Krebs, it's not unusual for the journalist to be targeted by the cybercriminals he is trying to expose. Earlier this month, he reported being hit by a 140 Gbps DDoS attack after exposing two Israeli individuals allegedly responsible for [operating a booter service](#) called vDOS.

Just before the latest attack, Krebs [detailed](#) the activities of a DDoS mitigation firm, which he discovered has a history of BGP hijacks and ties to questionable individuals.

DDoS attacks are the least of Krebs' worries. In the past, he was a [victim of swatting](#) and had [drugs sent to his home](#) by the individuals he had been investigating. On Wednesday, in addition to DDoS attacks, the blogger said the attackers had been trying to flood his Skype account with requests and his email inbox with subscriptions.

UPDATE. Brian Krebs has published a blog post with additional [details on the attack](#). According to the journalist, the attack does not appear to have relied on amplification, and a string found in some of the POST requests that hit his website referenced one of the alleged owners of vDOS.

Related Reading: ["Armada Collective" DDoS Threats Strike Again](#)

Related Reading: [Record Number of 100+ Gbps DDoS Attacks Hit in Q1 2016](#)

Eduard Kovacs ([@EduardKovacs](#)) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia's security news reporter. Eduard holds a bachelor's degree in industrial informatics and a master's degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs: