Hackers Begin Weaponizing TCP Middlebox Reflection for Amplified DDoS Attacks

thehackernews.com/2022/03/hackers-begin-weaponizing-tcp-middlebox.html

March 2, 2022

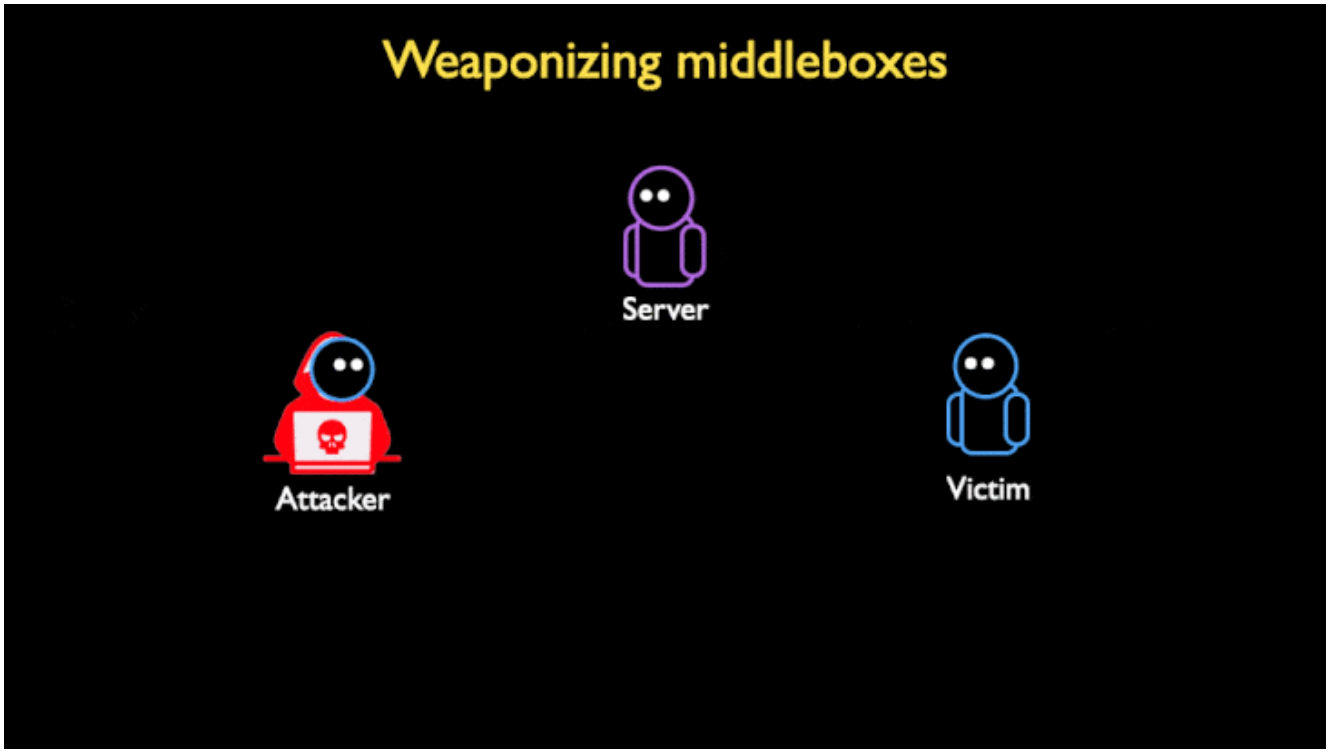
Distributed denial-of-service (DDoS) attacks leveraging a new amplification technique called **TCP Middlebox Reflection** have been detected for the first time in the wild, six months after the novel attack mechanism was presented in theory.

"The attack […] abuses vulnerable firewalls and content filtering systems to reflect and amplify TCP traffic to a victim machine, creating a powerful DDoS attack," Akamai researchers said in a report published Tuesday.

"This type of attack dangerously lowers the bar for DDoS attacks, as the attacker needs as little as 1/75th (in some cases) the amount of bandwidth from a volumetric standpoint," the researchers added.

A distributed reflective denial-of-service (DRDoS) is a form of distributed denial-of-service (DDoS) attack that relies on publicly accessible UDP servers and bandwidth amplification factors (BAFs) to overwhelm a victim's system with a high volume of UDP responses.

In these attacks, the adversary sends a flood of DNS or NTP requests containing a forged source IP address to the targeted asset, causing the destination server to deliver the responses back to the host residing at the spoofed address in an amplified manner that exhausts the bandwidth issued to the target.



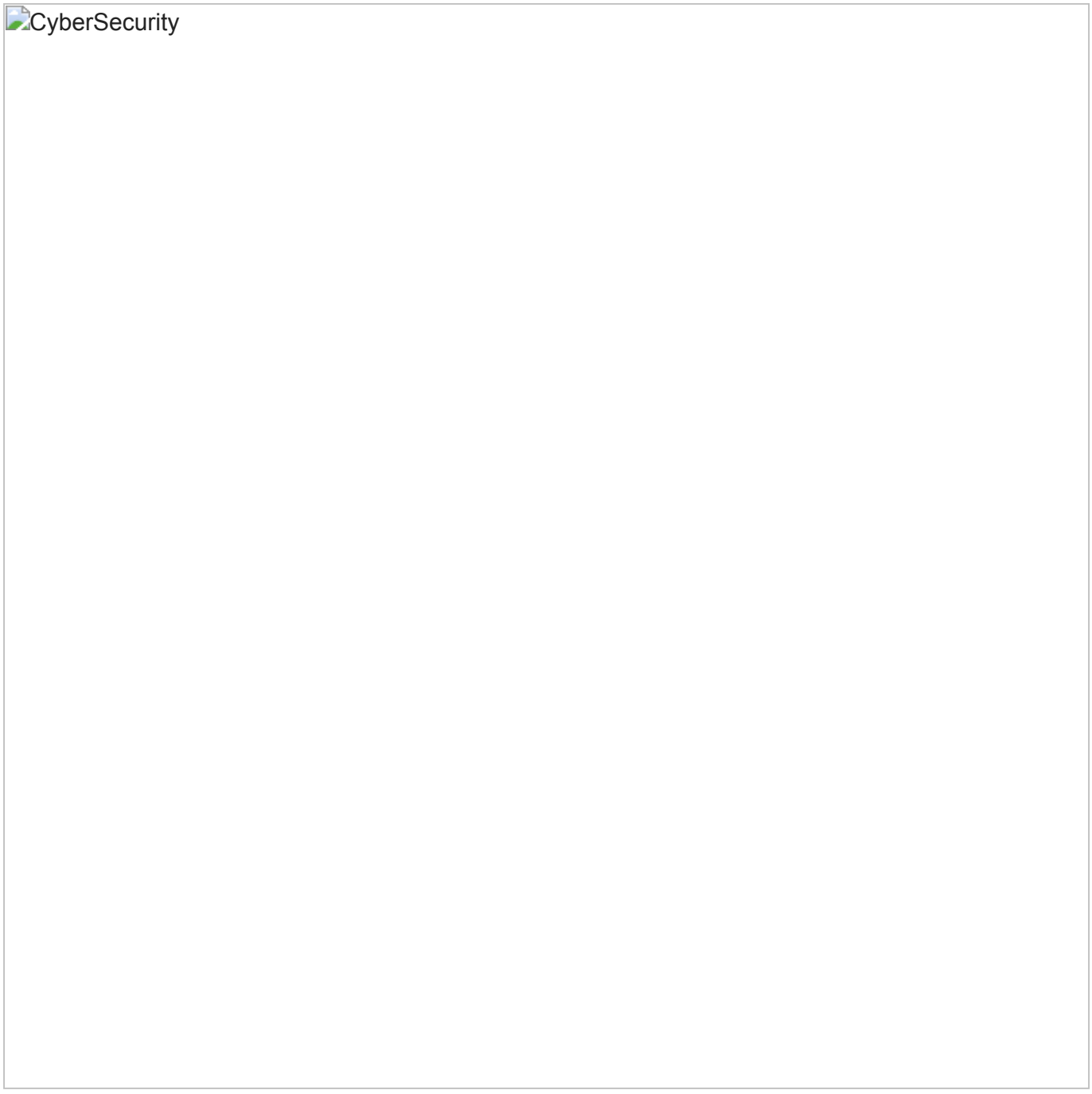
The development comes following an academic study published in August 2021 about a new attack vector that exploits weaknesses in the implementation of TCP protocol in middleboxes and censorship infrastructure to carry out reflected denial of service (DoS) amplification attacks against targets.

While DoS amplification attacks have traditionally abused UDP reflection vectors – owing to the connectionless nature of the protocol – the unconventional attack approach takes advantage of TCP non-compliance in middleboxes such as deep packet inspection (DPI) tools to stage TCP-

based reflective amplification attacks.

The first wave of "noticeable" attack campaigns taking advantage of the method is said to have occurred around February 17, striking Akamai customers across banking, travel, gaming, media, and web hosting industries with high amounts of traffic that peaked at 11 Gbps at 1.5 million packets per second (Mpps).

"The vector has been seen used alone and as part of multi-vector campaigns, with the sizes of the attacks slowly climbing," Chad Seaman, lead of the security intelligence research team (SIRT) at Akamai, told The Hacker News.



The core idea with TCP-based reflection is to leverage the middleboxes that are used to enforce censorship laws and enterprise content filtering policies by sending specially crafted TCP packets to trigger a volumetric response.

Indeed, in one of the attacks observed by the cloud security company, a single SYN packet with a 33-byte payload triggered a 2,156-byte response, effectively achieving an amplification factor of 65x (6,533%).

"The main takeaway is that the new vector is starting to see real world abuse in the wild," Seaman said. "Typically, this is a signal that more widespread abuse of a particular vector is likely to follow as knowledge and popularity grows across the DDoS landscape and more attackers begin to create tooling to leverage the new vector."

"Defenders need to be aware that we've moved from theory to practice, and they should review their defensive strategies in accordance with this new vector, which they may be seeing in the real world soon," Seaman added.