New American

Written by **James Donlon** on March 8, 2018

Two Online Services Survive Record-breaking Cyberattacks

On February 28, GitHub, a major software-development and sharing platform and the largest open-source online community, was the victim of the largest-ever DDoS (Distributed Denial of Service) attack. DDoS is a type of attack in which the perpetrator overloads an online service by bombarding it with traffic from multiple sources. The server usually cannot handle the incoming traffic, and will not be able to function properly, and usually crashes. DDoS attacks usually utilize "bot nets," networks of infected computers which are controlled remotely without the owners even knowing. The attackers then use these botnets, which can number as many as millions of computers, to carry out the DDoS attack on the victim. DDoS attacks have been around for a while and all major online sites and services prepare for such attacks.

Last Wednesday's attack on GitHub was unique, however. DDoS attacks usually peak at a few hundred gigabytes of data per second, if that. GitHub was attacked with 1.35 terabytes per second. One terabyte is one-thousand gigabytes. That's a lot of data. This was the biggest attack ever publicly announced. Incredibly, though, the attack was also a massive failure. Within 10 minutes, GitHub's Internet traffic was "scrubbed" (analyzed and filtered) to find and block the malicious data. Within a few more minutes, GitHub had completely thwarted and survived the massive attack.

How were the attackers able to bombard GitHub with so much data? Herein lies the scary part of the attack. The DDoS was launched not through a botnet, but through something called memcached servers. Without going into unnecessary detail, memcached servers are meant to speed up online databases and web applications. An attacker can send a packet of data to a memcached server through an exploit, which will return with an exponentially larger response. Thus, the attackers sent loads of data, every few seconds, and the resulting 1.35 terabytes of traffic per second overloaded GitHub's servers.

This attack was a massive record. However, five days later, the record was already broken. On Monday, an unidentified service provider was attacked by another DDoS; this time the traffic was 1.7 terabytes per second of traffic. While there are fewer details regarding this attack, it, too, was mitigated quickly and no major damage was done. Obviously, however, this is the newest trend of cybercrime, and will surely continue.

So while the method is actually somewhat simple, the more serious problem is the accessibility of the

memcached servers. According to *Wired*, thousands of these servers are exposed online without any serious protection or authentication. This is a big problem. The conclusion many are reaching from the attack is that memcached servers need to be at least secured, or ideally taken completely off the public Internet. Until this happens, the attacks will very likely continue — and very possibly grow, as we have already seen.

So while these two attacks were the largest the world has seen, they will certainly not be the last. Once cybercriminals find such a massive method of attack, others will soon adopt those same tactics. Anyone with an Internet connection and the proper knowhow can access a memcached server and amplify traffic by 51,000 times, wreaking havoc on the target of his choice. So far, there are no known motives for the attacks, but such is the nature of these types of crimes: hackers showing off their skills to gain a reputation.

The overlooked aspect of the attacks, which should be emphasized perhaps as much as the massive scale of the attack itself, is the incredibly swift response and effective mitigation. The GitHub services experienced outages, but the worst part was over in 10 minutes. This is a testament to serious cybersecurity understanding and planning. If this happened a few years ago, the results would likely have been very different. Some DDoS attacks, just a few years ago, could last days or weeks, because institutions did not adequately prepare for such attacks as they do today.However, since people are now quite aware of the serious threats that individuals, and especially institutions, face online, GitHub totally thwarted the attack in less than half an hour. So yes, the attacks are massive. They are the biggest ever. But they failed.

In order to completely stop — and hopefully prevent — these attacks, however, memcached servers should either be taken off of the public Internet or at least properly secured. They are easily weaponized and, as such, are a liability to the Internet. Otherwise, this type of cyberattack will gain more popularity and could become a daily occurrence.