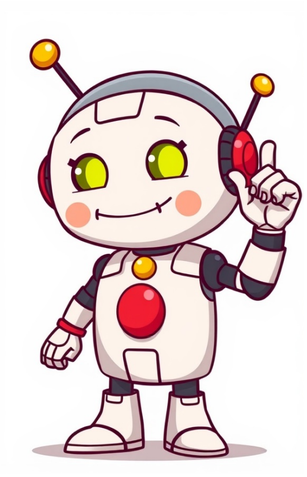
Click to prove you're human



The record-breaking distributed denial-of-service (DDoS) attack, mitigated by Cloudflare, reached unprecedented levels with a peak of 22.2 terabits per second (Tbps) and 10.6 billion packets per second (Bpps). This massive assault was not only enormous in volume but also had a lasting impact on the victim's system resources, equivalent to streaming one million 4K videos simultaneously for a brief 40 seconds. The packet rate of 10.6 Bpps translates to roughly 1.3 web page refreshes per second from every person on the planet, making it extremely challenging for firewalls, routers, and load balancers to process requests. Cloudflare's mitigation efforts successfully blocked this hyper-volumetric DDoS attack, which is considered one of the largest ever recorded. Cloudflare has been dealing with a surge in record-breaking DDoS attacks, including the massive 11.5 Tbps and 5.1 Bpps attack that occurred just three weeks ago and another that peaked at 7.3 Tbps two months prior. The company warned earlier this year about an unprecedented number of DDoS attacks, highlighting the growing threat in the cybersecurity landscape. Researchers from XLab, a division of Qi'anxin, attributed the 11.5 Tbps attack to the AISURU botnet, which has infected over 300,000 devices worldwide and targets various vulnerabilities in IoT devices. The recent attack demonstrates the increasing sophistication and scale of DDoS attacks, emphasizing the need for robust mitigation strategies and cybersecurity measures. Cloudflare's ability to autonomously block these massive attacks highlights its capabilities in protecting against such threats, but it also raises concerns about the limits of their mitigation capacity. As the frequency and magnitude of DDoS attacks continue to rise, organizations must remain vigilant and proactive in addressing this growing threat.The enterprising hackers who dare to attempt such a feat are likely to be rewarded with notoriety, but at what cost? Cloudflare has confirmed that its systems successfully stopped a record-breaking distributed denial-of-service (DDoS) attack that reached unprecedented levels of infamy. The attack, which lasted only 40 seconds, equaled streaming one million 4K videos simultaneously. The volume involved was massive, with the attack reaching 22.2 terabits per second and 10.6 billion packets per second. This figure is comparable to every person on Earth refreshing a web page once a second. Cloudflare's systems detected and mitigated the incident autonomously without manual intervention. This achievement sets a new bar for DDoS assaults, highlighting the rapid escalation of attack sizes over the past few months. The company did not disclose any details about the source or target of the attack, but confirmed that it was stopped before any lasting damage could occur. Mitigation of such an attack is a complex task, as firewalls and load balancers struggle to handle high request counts. In April, Cloudflare noted that 2025 was on track for record levels of DDoS activity. The latest incident is another example of the growing threat landscape. Cloudflare's systems have already blocked multiple record-breaking attacks this year, demonstrating their ability to stay ahead of the threats. Cloudflare Mitigates Record-Breaking 22.2 Tbps DDoS Attack ========== Cloudflare has mitigated a new record-breaking distributed denial-of-service (DDoS) attack that peaked at a staggering 22.2 terabits per second (Tbps) and 10.6 billion packets per second (Bpps). This attack more than doubled the previous UDP flood record of 11.5 Tbps, highlighting the accelerating capabilities of botnets and the sophistication of modern attackers. The attack unfolded in a “hit-and-run” fashion, lasting approximately 40 seconds, with attackers combining multiple vectors to maximise disruption within a very narrow window. The sheer scale of the traffic indicates the use of massive botnets composed of compromised servers and Internet-of-Things devices, orchestrated to saturate network pipes and exhaust server resources. Technical details reveal a peak of 10.6 Bpps, indicating that the traffic was not just volumetrically extreme but also highly packet-intensive. UDP amplification and reflection techniques appear to have been leveraged to generate the surge, stressing network hardware and testing the limits of edge routers and firewall appliances. The frequency of record-breaking DDoS attacks is a growing concern, with this event marking a sharp departure from the past. Two to three years ago, large-scale DDoS incidents of this magnitude were rare, with perhaps one or two significant events each year.FastNetMon is a leading solution in network security that offers advanced DDoS detection and mitigation capabilities with real-time analytics and rapid response abilities. It helps organisations identify potential attacks early on and safeguards their infrastructure from evolving threats. FastNetMon Advanced seamlessly integrates with Cloudflare Magic Transit, making it possible to mitigate DDoS attacks with ease. When an attack is detected, FastNetMon can automatically reroute traffic to Cloudflare's global scrubbing centres, ensuring that only malicious traffic is sent for cleaning while legitimate traffic continues uninterrupted. Cloudflare recently reported mitigating the largest recorded distributed denial-of-service (DDoS) attack ever observed. This hyper-volumetric assault reached an astonishing 22.2 terabits per second and 10.6 billion packets per second, more than double the size of any previous DDoS event. The record-breaking attack lasted only about 40 seconds but caused significant disruption. The assault was a multi-vector attack that combined various techniques to amplify its impact. Such attacks are typically launched from massive botnets, networks of compromised computers and IoT devices, which flood a target's servers with an overwhelming amount of traffic, rendering services unavailable to legitimate users. Cloudflare's systems autonomously detected and blocked the attack without any human intervention. This successful defense highlights the growing need for automated cybersecurity solutions powered by machine learning to counter threats that operate at machine speed. Legacy DDoS "scrubbing" centers are often ill-equipped to handle attacks of this magnitude and velocity, requiring manual analysis and traffic redirection. Cloudflare's global network was able to absorb and neutralize the malicious traffic at the edge, close to its source. As attackers continue to refine their methods and expand their botnets, the frequency and intensity of hyper-volumetric attacks are expected to rise. This emphasizes the importance for businesses to evaluate whether their security provider has the necessary network capacity and automated technology to withstand such onslaughs.