The rise of “super-botnets”: FastNetMon reveals what’s behind this year’s record-shattering DDoS attacks

With attacks reaching unprecedented scale, FastNetMon warns that a commercialised global botnet — Aisuru — is straining the internet infrastructure relied on by millions worldwide.

London, United Kingdom Dec 13, 2025 (Issuewire.com) - FastNetMon, a leading provider of network security solutions, reports that record-breaking distributed denial-of-service (DDoS) attacks in 2025 are powered by Aisuru, a rapidly evolving global botnet. Leveraging an army of compromised devices — from routers to cameras — Aisuru has executed some of the largest attacks ever recorded, creating new challenges for internet stability.

“Hyper-scale attacks like those powered by Aisuru aren’t just isolated incidents anymore. They’re a warning that the internet’s resilience is being tested on a daily basis, and it affects every service we rely on — from email and entertainment to finance and healthcare,” said **Pavel Odintsov, Founder of FastNetMon**.

Unlike earlier attacks, which were slow and small, these assaults are **fast, intense, and enormous in scale**. One recent incident generated enough traffic to stream tens of millions of high-definition movies at once, illustrating the extraordinary strain super-botnets can place on networks worldwide.

DDoS attacks are growing exponentially

DDoS attacks have evolved dramatically over the past two decades. Early attacks in the 2000s, measured in **megabits or gigabits per second**, could disrupt a single website temporarily. By 2015–2020, **terabit-level floods** appeared, challenging even the largest providers.

Now, multi-terabit assaults are becoming frequent. FastNetMon’s data shows that attack volumes are

rising faster than many defences can adapt, creating persistent risks for everyday internet users and businesses alike.

The hidden ripple effect

Attacks orchestrated by super-botnets like Aisuru originate from a large pool of compromised devices, creating massive traffic surges that ripple across the internet. This is especially critical in regions like Latin America, where international network capacity is limited. When a multi-terabit attack crosses overseas links, it can slow services for everyone - not just the intended target - affecting streaming, banking, and business operations.

“The internet is a shared ecosystem. Protecting it isn’t just a technical challenge — it’s essential to ensuring that the services people depend on every day remain reliable,” added **Pavel Odintsov, Founder of FastNetMon**.

Rapid detection and mitigation solutions, such as FastNetMon, are now critical for networks to **detect attacks in real time and prevent disruptions from spilling across networks**. Protecting digital operations now requires **global visibility, rapid response, and collaboration across providers and regions**, ensuring that the internet remains collectively resilient even in the face of record-breaking attacks.

Media Contact

FastNetMon

*********@fastnetmon.com

Source : FastNetMon

See on IssueWire