The Internet is (once again) awash with IoT botnets delivering record DDoSes

We're only three weeks into 2025, and it's already shaping up to be the year of Internet of Things-driven DDoSes. Reports are rolling in of threat actors infecting thousands of home and office routers, web cameras, and other Internet-connected devices.

Here is a sampling of research released since the first of the year.

Lax security, ample bandwidth

A post on Tuesday from content-delivery network Cloudflare reported on a recent distributed denial-of-service attack that delivered 5.6 terabits per second of junk traffic—a new record for the largest DDoS ever reported. The deluge, directed at an unnamed Cloudflare customer, came from 13,000 IoT devices infected by a variant of Mirai, a potent piece of malware with a long history of delivering massive DDoSes of once-unimaginable sizes.

The same day, security company Qualys published research detailing a "large-scale, ongoing operation" dubbed the Murdoc Botnet. It exploits vulnerabilities to install a Mirai variant, primarily on AVTECH Cameras and Huawei HG532 routers. Late Tuesday afternoon, searches like this one indicated devices on more than 1,500 IP addresses were compromised, up from a figure of 1,300 reported a few hours earlier by Qualys. These devices are also waging DDoSes. It's unknown if

Cloudflare and Qualys are reporting on the same botnet.

Last week, security company Trend Micro said it also found an IoT botnet. The botnet, which is driven by variants of Mirai and a similar malware family known as Bashlite, has been delivering large-scale DDoSes since the end of last year, primarily to targets in Japan.

A report early last week from security firm Infoblox revealed a botnet comprising 13,000 devices—mostly routers manufactured by MikroTik—that researchers likened to “a large cannon, poised and ready to unleash a barrage of malicious activities.” The primary activity Infoblox has observed from this botnet is a flood of malicious spam emails that attempt to trick recipients into executing malicious file attachments.

https://arstechnica.com/security/2025/01/the-internet-is-once-again-awash-with-iot-botnets-delivering-record-ddoses/