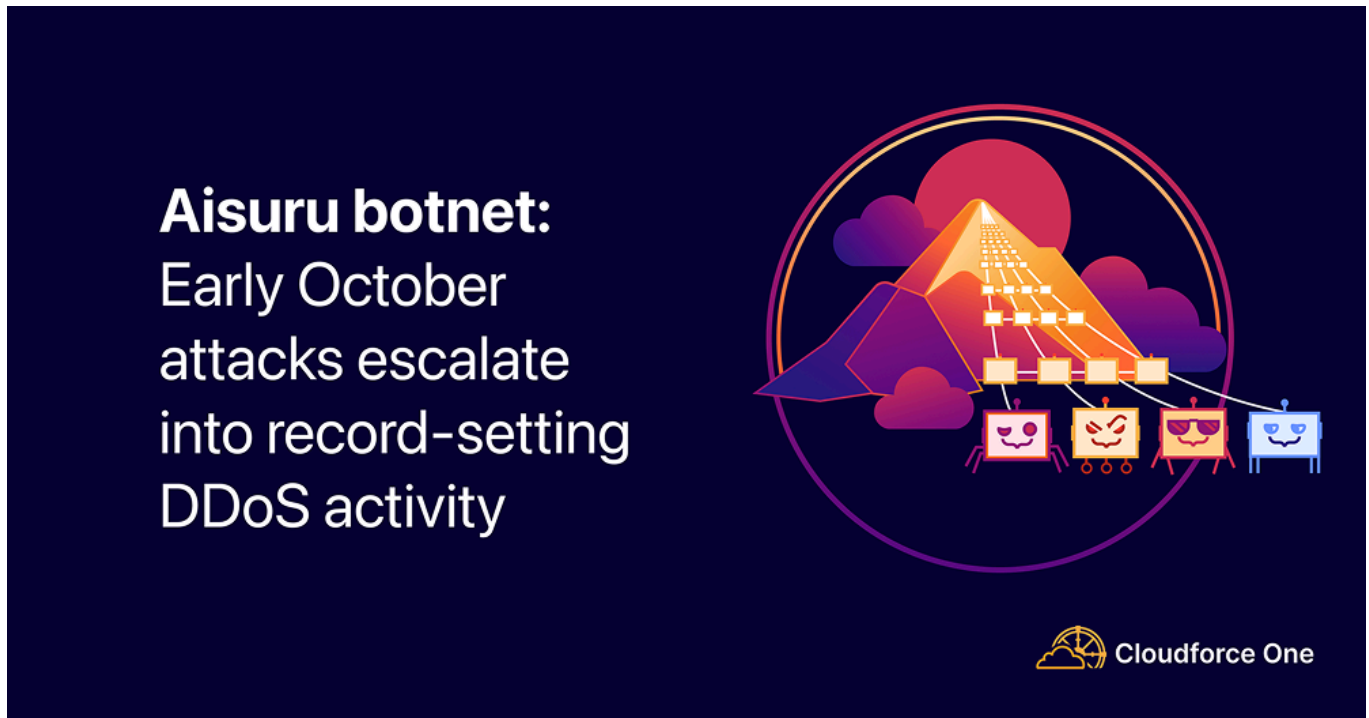


Aisuru botnet: Early October attacks escalate into record-setting DDoS activity

 cloudflare.com/en-au/threat-intelligence/research/report/aisuru-botnet



On October 31st, 2025, Cloudflare’s network detected the largest UDP DDoS attacks of the year—peaking at 29.7 Tbps. The attacks were powered by a fast-growing Aisuru botnet, composed of infected hosts ranging from public-cloud virtual machines to routers, security appliances (including firewalls), and Internet of Things (IoT) devices such as internet-connected cameras. Since early October, the botnet’s footprint has expanded sharply, amplifying the scale and intensity of attacks. While our telemetry reveals that a multitude of industries were targeted, the Telecommunications industry by far has borne the brunt of these attacks, accounting for 73% of observed activity.

This article provides a preliminary summary of what we’ve seen so far: how Aisuru evolved into record-setting volumes, what telemetry shows about its infrastructure and growth, and how Cloudflare’s systems responded automatically in real time. We also shed light on how DDoS attacks in general have escalated massively in the past year, and how organizations can protect themselves in this new era of hyper-volumetric attacks. Our analysis is still developing under Cloudforce One, and findings here reflect current evidence from traffic telemetry and incident logs gathered between late September and early November.

What is Aisuru?

Aisuru is an IoT-based botnet with approximately 500,000 compromised hosts, a force that doubled in size in just four weeks. Its operators leverage a multi-pronged infection strategy, including an alleged [firmware supply-chain compromise](#), to continuously grow their network of devices infected with the Aisuru malware and its [variants](#), [kitty](#) and [AIRASHI](#).

The primary and most visible capability of the Aisuru botnet is its ability to generate DDoS attacks of a magnitude previously thought to be theoretical. The botnet has consistently set new records for attack volume, escalating from 6.35 Tbps in May 2025 to a peak of 29.7 Tbps by October 2025. The sheer scale of these attacks is difficult to comprehend. A 12 Tbps flood, for instance, is about the bandwidth of 56,075 typical U.S. residential internet connections being directed at a single target simultaneously. Such volumes are sufficient to overwhelm the infrastructure of all but the most well-prepared global network providers.

The Aisuru campaign observed by Cloudflare leverages a popular method: hyper-volumetric and ultra-sophisticated UDP carpet-bombing DDoS attacks. The highly distributed UDP attacks sprayed traffic across thousands of ports per second, attempting to overwhelm targets with a flood of junk connectionless packets. At the same time, the actor heavily randomized packet attributes, making precise detection and mitigation nearly impossible for simple mitigation systems or ACL-based defenses.

Aisuru employs a tactic in which attacks surge from zero to maximum intensity almost instantly, sustaining peak traffic for only 30–70 seconds. This short, high-impact burst is designed to maximize damage while minimizing detection, leveraging both extreme brevity and heavy traffic randomization.

Aisuru hyper-volumetric DDoS attack analysis

On October 31, 2025, the Aisuru botnet launched a full-scale, coordinated assault, with Cloudflare’s network detecting one of the largest and most sustained IoT-driven DDoS attacks on record. Devices affected included routers (e.g., Totolink, Nexxt, Linksys), DVRs (Digital Video Recorders), internet-connected cameras, gateway/firewall appliances (e.g., Zyxel’s USG FLEX, VPN, and ZyWALL/USG), and cnPilot networking devices (from Cambium Networks).

This carpet-bomb UDP attack—the largest DDoS attack in history at 29.7 Tbps—was mitigated autonomously by Cloudflare.

Aisuru bombarded UDP packets at an average of 15,000 destination ports per second, peaking at 34,000 thousand per second in its initial spike. Cloudflare also observed multiple flood patterns in parallel—including TCP SYN floods and TCP ACK floods. Some instances targeted single IPs (e.g., /32) and others struck broader /24 subnets, suggesting that the bot operators were tuning parameters dynamically.

The attack also randomized additional packet attributes in an attempt to evade detection, including but not limited to TTL, source ports, checksums, and option fields. Traffic originated from an average of 17,000 source ASNs per second, peaking at 45,000 per second, and was mitigated by Cloudflare data centers across 113 countries.

Hyper-volumetric attack insights

Since mid-2024, Cloudflare has observed an unprecedented increase in the size of hyper-volumetric DDoS attacks, predominantly UDP carpet-bombing attacks. The DDoS attack world record, for example, surged from 4.2 Tbps in October 2024 to 29.7 Tbps in October 2025—a staggering 707% increase YoY.

Cloudflare has autonomously mitigated over 3,300 hyper-volumetric DDoS attacks launched by Aisuru since the start of 2025, an average of 334 hyper-volumetric DDoS attacks per month and 11 attacks every single day:

A sample of the largest DDoS attacks mitigated by Cloudflare, Sept 2024 - Oct 2025

Cloudflare mitigated 1,304 hyper-volumetric attacks in Q3 2025, an increase of 54% QoQ. These include the world-record breaking 29.7 Tbps Aisuru DDoS attack and a 14.1 billion packets per second (Bpps) DDoS attack:

Distribution of hyper-volumetric network-layer attacks, Jan 2025 - Oct 2025

Overall, the number of attacks gradually increased steadily throughout the year, with July reaching 522 attacks in total—an average of 17 attacks per day:

Hyper-volumetric DDoS attacks by quarter, Q1 2025 - Q3 2025

In September and October, we saw the aforementioned bombardment of hyper-volumetric attacks including an increase in packet-rate intensive attacks:

Hyper-volumetric DDoS attacks by month, Jan 2025 - Oct 2025

For a more comprehensive analysis of the evolving threat landscape of DDoS attacks based on recent data from the [Cloudflare network](#), see Cloudflare's [2025 Q3 DDoS Threat Report](#).

Aisuru IP analysis (September and October)

Early IP analysis showed that 74% of attacking IPs were active for two days or less, suggesting high churn and that IP-based blocking alone would not remain effective for long.

Pareto analysis of Aisuru attack IPs since early September 2025 showing most Aisuru-controlled hosts appeared briefly before disappearing

Through late September, the botnet demonstrated high volatility—frequent bursts, limited persistence, and rapid replacement of IPs—but by early October, that pattern shifted.

Between October 1 and October 9, Cloudflare's mitigation telemetry showed a marked increase in stability and persistence across attacking IPs. New IPs continued joining daily, but the proportion of repeat offenders grew from 43% to nearly 87% of observed traffic within 10 days—evidence that Aisuru was stabilizing its botnet core.

Persistence of Aisuru attack IPs on October 9, 2025 – compared to late September, a larger share of IPs remained active for several days

By October 6, the botnet's capacity had expanded dramatically. Cloudflare mitigated a hyper-volumetric DDoS attack peaking at 29.7 Tbps and a 14.1 Bpps attack on October 7th, one of the largest events seen to date. At the same time, IP segmentation graphs showed newly observed IPs joining en masse during the period of October 3 through October 9, pointing to active device recruitment and command infrastructure expansion:

DDoS volume segmented by IP first-seen date. New color bands after October 3, 2025 reflect a surge of freshly recruited IoT devices entering Aisuru's botnet.

Aisuru TTPs

Analysis of the Aisuru attacks reveals a set of highly destructive and technically advanced tactics, techniques, and procedures (TTPs). Rather than relying on a single method, the operators employed a broad, customizable arsenal of attack variants. Cloudforce One is aware of at least eight flood types (including UDP, TCP SYN, and TCP ACK), each with its own configurable parameters—such as whether to target a fixed or randomized destination port, or whether to strike a single host or an entire subnet. Cloudforce One also conducted analysis of a key malware sample (`nx86_64.elf`, 08717d85a8a296279c2d2b792a33714d216a9de1950173d603222f78da9b9ca5), which revealed a sophisticated design focused on stealth, resilient command and control (C2), and advanced payload capabilities.

Command and Control

Aisuru does not rely on simple, hardcoded IP addresses for its C2 infrastructure. Instead, it pulls its C2 IPs from DNS TXT records, a technique that makes the botnet highly resilient to takedowns. An operator can simply update the DNS record to redirect the entire botnet, rendering IP-based blocklists ineffective.

To further conceal this, the IPs are obfuscated using a custom encoding scheme: the IP address is converted to hex, XORed with the constant `0xCafEBABE`, and finally Base64 encoded. This obfuscation is designed to bypass simple text-based security filters. The initial DNS callout observed was to the domain `dvrxpert.tiananmensquare1989[.]su`. Cloudflare actioned this domain and all other identified domains controlled by the actor.

Advanced encryption model

The malware employs a robust, two-tiered encryption strategy designed to protect both its internal configuration and its external C2 traffic. Internally, a hardcoded RC4 key (`PJbiNbbeasddDfsc`) is used to decrypt embedded strings, including C2 URLs, operational parameters, and other configuration data.

More significantly, all C2 communications are secured using ChaCha20 encryption. For each new connection, the malware and its C2 server exchange 64KB of random data to derive a unique session key. This “per-session keying” ensures that every connection is cryptographically isolated: data captured from one session cannot be used to decrypt any other. As a result, network defenders are unable to build reusable signatures or decrypt historical traffic, greatly complicating detection and forensic analysis.

Host-based stealth and anti-analysis

On an infected host, the malware immediately forks a child process and renames itself to mimic a common Linux daemon, such as `telnetd`, `udhcpd`, `ntpcclient`, or `klogd`. This masquerading enables it to blend in with legitimate system processes, helping it evade detection during routine administrative checks.

The binary also employs active anti-analysis techniques. It enumerates system CPU information (via `/sys/devices/system/cpu`) and inspects process and CPU statistics (via `/proc/stat` and `/proc/cpuinfo`). These checks are designed to detect signs of sandboxing or virtualization commonly used by security researchers, allowing the malware to terminate or modify its behavior to impede analysis.

Advanced payload capabilities

The `nx86_64.elf` sample contains detailed functions for parsing incoming HTTP requests, meticulously splitting URLs into their constituent parts (host, path, query, fragment). In addition, Aisuru uses STUN (Session Traversal Utilities for NAT) to identify its public-facing outbound communication. This enables infected devices to accurately register their public IPs with C2 servers.

Aisuru victimology

The Aisuru campaigns primarily targeted Cloudflare customers using DNS and HTTP services, along with a smaller number of other major Internet providers. The profile of Aisuru's activity—focusing on DNS resolvers and API-heavy services—aligns with botnets used to disrupt services with large public endpoints.

The campaign's scope and target selection mainly focused on Telecommunications, with over 60% of attacks (many of which were for testing the botnet) aimed at this industry, followed by Information Technology and Services (12.7%), Gaming (7.8%), and Cybersecurity (6.4%). In terms of geographic targets, Aisuru mainly focused on the United States (76%) followed by China (10%) and Hong Kong (5%).

Aisuru attribution

While precise attribution remains under investigation, [public reporting](#) indicates that the Aisuru botnet is purportedly run by a group of three individuals that operate under the pseudonyms Snow, Tom, and Forky. In a May 2025 [article](#) about Aisuru's then-record 6.3 Tbps attack, Forky—identified as a 21-year-old man from Sao Paulo, Brazil—acknowledged contributing to Aisuru's development and marketing but denied any involvement in launching the attacks. An anonymous source further alleged that Tom was responsible for vulnerability discovery, while Snow handled the botnet's development.

The group has also stated that they carry out highly destructive attacks on ISPs “for fun.” Their domain-naming patterns reinforce this posture: alongside politically themed domains (e.g., `tiananmensquare1989[.]su`), the actors have registered sexually explicit and deliberately provocative names. This combination suggests an intent to shock, troll, or mislead analysts rather than signal any genuine ideological or geopolitical alignment, making these domains more likely to be false flags than meaningful indicators of motivation.

How Cloudflare mitigated the attacks

The distributed attack randomized various packet attributes in an attempt to evade defenses, but Cloudflare's mitigation systems detected and mitigated all the attacks, including this one, fully autonomously. Read more on [How Cloudflare mitigates hyper-volumetric DDoS attacks](#).

The following network-layer DDoS rules were most effective during mitigation:

- Enable [high-sensitivity](#) DDoS Managed Rules, especially those targeting UDP floods and known-bad-source traffic.

- Use [Magic Firewall](#) expressions to restrict inbound traffic to expected ports and protocols.
 - Enforce a positive security model: [Create rules](#) to allow the type of traffic you are expecting to the destination IP/ports you are expecting (if you are able to [form an expression](#) to describe it with the [Magic Firewall fields](#)) followed by a “deny all” rule at the bottom of the list.
 - If a positive security model is not possible, then enforce a negative security model: Block unwanted traffic or traffic you do not expect to receive (with emphasis on the UDP protocol) to destination IP addresses/ranges, and ports/port ranges. For example, blocking UDP traffic to IPs and ports that are not expecting UDP traffic.
- Enterprise customers should ensure [Adaptive DDoS protection](#) is enabled and that override rules are in “Block” mode rather than “Log”.
- Monitor for short-lived spikes in traffic from newly observed IPs; review logs for patterns of randomized subdomain queries or HTTP floods with short-lived connections.

Recommendation for service providers

Register your ASN with Cloudflare to receive free threat intelligence about DDoS attacks originating from your networks. The Free ISP DDoS Botnet threat feed is simple to set up, and using the API you can retrieve a list of IPs from within your network that we’ve seen participate, with high confidence, in launching DDoS attacks.

IOCs

Type	Indicator	Description
SHA256 Hash	08717d85a8a296279c2d2b792a33714d216a9de1950173d603222f78da9b9ca5	nx86_64.elf (Main sample analyzed)
SHA256 Hash	201d872e05f45062f3b18f1cb2bca7d5fe3811e7e6d4b8616d565a011fba091d	skid.armv7l.elf
SHA256 Hash	7a5a5c813d636d96906fb4bf8f76c7f296a467dca756e92450f32dc69d781b71	armv4l.elf
SHA256 Hash	50d3806f47d3f701d5f1f93bf39f827f936e3d1f43fa2cd8408db9655d53fb83	armv7l.elf
SHA256 Hash	90e3b997161e33c6485b48182073a864dd3d0775ab96cadbf1b7c9dd4821c6d1	aarch64.elf

Type	Indicator	Description
Domain	dvrxpert.tiananmensquare1989[.]su	Initial C2 callout domain for nx86_64 sample
Encryption Key	PJbiNbbeasddDfsc	Hardcoded RC4 key for decrypting internal strings/config
Encryption Key	0xCAFEBAFE	XOR key used to encode C2 IPs in DNS TXT records
Host Artifact	telnetd, udhcpd, inetd, ntpclient, watchdog, klogd, upnnp, dhclient	Malware masquerades as these process names
Host Artifact	/sys/devices/system/cpu, /proc/stat, /proc/cpuinfo	File path used in anti-analysis checks

Domains

ballsack.14emeliaterracewestroxburyma02132[.]su

a.6mv1eyr328y6due83u3js6whtzuxfyhw[.]su

eviate-lives-at.14emeliaterracewestroxburyma02132[.]su

2.tiananmensquare1989[.]su

approach.dvrinside[.]net

coerece.dvrinside[.]net

Domains

dvrinside[.]net

lane.dvrinside[.]net

ministry.dvrinside[.]net

s.cuckstudios[.]su

arf.santasbigcandycane[.]ru

re.santasbigcandycane[.]ru

nfs.santasbigcandycane[.]ru

busybox.feds2door[.]su

feds2door[.]su

updatetoto[.]tw

lane.ilovegaysex[.]su

approach.ilovegaysex[.]su

ministry.ilovegaysex[.]su

coerece.ilovegaysex[.]su

epson.ilovegaysex[.]su

ilovegaysex[.]su

stevenfromcoinbase.fk3[.]su

6mv1eyr328y6due83u3js6whtzuxfyhw[.]su

dvrxpert.tiananmensquare1989[.]su

Domains

testlmaololwtf.tiananmensquare1989[.]su

14emeliaterracewestroxburyma02132[.]su

C2 IPs decoded from TXT records

45[.]154[.]96[.]24

45[.]138[.]16[.]234

45[.]80[.]158[.]144

45[.]80[.]158[.]129

45[.]43[.]57[.]186

45[.]43[.]57[.]167

161[.]35[.]159[.]168

164[.]90[.]174[.]64

167[.]172[.]160[.]49

167[.]172[.]190[.]98

167[.]99[.]52[.]96

193[.]26[.]115[.]154

193[.]26[.]115[.]48

194[.]58[.]38[.]57

185[.]241[.]208[.]197

185[.]241[.]208[.]165

C2 IPs decoded from TXT records

193[.]233[.]84[.]64

193[.]233[.]84[.]67

193[.]233[.]84[.]65

193[.]233[.]84[.]68

193[.]233[.]84[.]71

193[.]233[.]84[.]76

193[.]233[.]84[.]73

193[.]233[.]84[.]63

193[.]233[.]84[.]19

178[.]128[.]227[.]241

209[.]38[.]218[.]0

77[.]110[.]112[.]132

77[.]110[.]112[.]4

77[.]110[.]112[.]5

78[.]153[.]149[.]249

65[.]108[.]5[.]46

68[.]183[.]179[.]103

68[.]183[.]206[.]140

88[.]151[.]192[.]129

C2 IPs decoded from TXT records

81[.]19[.]140[.]41