RED BUTTON
DDoS Experts

Red Button DDoS Threat Pulse - June 2026

13/07/2026

CONFIDENTIALITY & PROPRIETARY

DDoS Threat Pulse

Your monthly briefing on the DDoS threat landscape

June 2026 Edition

Red Button's Threat Intelligence team continuously researches the evolving DDoS attack ecosystem - tracking new attack techniques, emerging botnets' infrastructures, and the threat actors behind them. DDoS Threat Pulse is our way of sharing that intelligence with you: a monthly briefing on the developments we believe matter most to organizations. Our goal is to help you understand what's changing in the DDoS landscape and use that insight to inform your own security posture - whether that means adjusting or hardening your DDoS protection configuration, or simply knowing what to ask your team. We hope you find it useful, and we welcome your feedback.

IN THIS ISSUE

- A newly disclosed vulnerability that lets a single machine - no botnet required - take a major website offline in seconds
- A World Cup-timed flash DDoS attack against a European betting platform - and what it says about event-driven risk
- A newly discovered botnet built from thousands of outdated home and office routers - and why it matters even though it isn't (yet) being used for DDoS

One machine, No Botnet: A New Way to Take Down a Website

In early June, security researchers disclosed a new technique - nicknamed 'HTTP/2 Bomb' - that lets a single attacker take a website offline in seconds, using nothing more than an ordinary home internet connection. No botnet. No rented attack infrastructure. No coordination with other machines at all.

That's a meaningful departure from how denial-of-service attacks have typically worked. The technique exploits a flaw in how many widely used web servers - including some of the most common software powering websites worldwide - handle a core part of modern web traffic. In short: a specially crafted connection tricks the server into holding open far more memory than it should, until it runs out and the server stops responding. Researchers demonstrated that a single connection could exhaust tens of gigabytes of server memory in well under a minute.

When researchers scanned the internet for servers running the vulnerable configuration, they found more than 880,000 exposed. The good news: major vendors moved quickly, with the most widely used web server software patched within days and others addressed through their normal June security updates - though not every affected product had a fix available immediately. One more detail worth knowing: researchers found this vulnerability with the help of an AI coding assistant, a small but telling sign of how AI is starting to change not just how organizations defend against attacks, but how new attack techniques get discovered.

WHAT THIS MEANS FOR YOU

This is worth a direct conversation with whoever manages your web servers, load balancers, or CDN configuration. Ask them to confirm three things: which web server software and version your internet-facing systems are running, whether it's been updated since early June, and whether HTTP/2 is enabled. If you're not sure who owns that internally, your Red Button contact can help.

A Flash DDoS Attack Timed to the World Cup

As the 2026 FIFA World Cup kicked off, security researchers at DataDome observed a sharp rise in DDoS and bot activity against sports-betting platforms - a sector that sees enormous, predictable traffic spikes around major sporting events. One major European betting platform was hit particularly hard.

In the days leading up to the tournament, malicious traffic against the platform had already climbed to around 200,000 blocked requests a day. Then, on the eve of the opening match, attackers launched what researchers call a 'flash DDoS': a very short, very intense burst of traffic designed to overwhelm a target before protections have time to react.

Over the following three weeks, the platform absorbed nearly 19 million malicious requests in total. Researchers traced most of the attack traffic to a single Russia-based hosting and proxy provider, though no hacktivist group or nation-state actor publicly claimed responsibility - this appears to have been an opportunistic attack that took advantage of the tournament's visibility and traffic surge, rather than a politically motivated campaign.

WHAT THIS MEANS FOR YOU

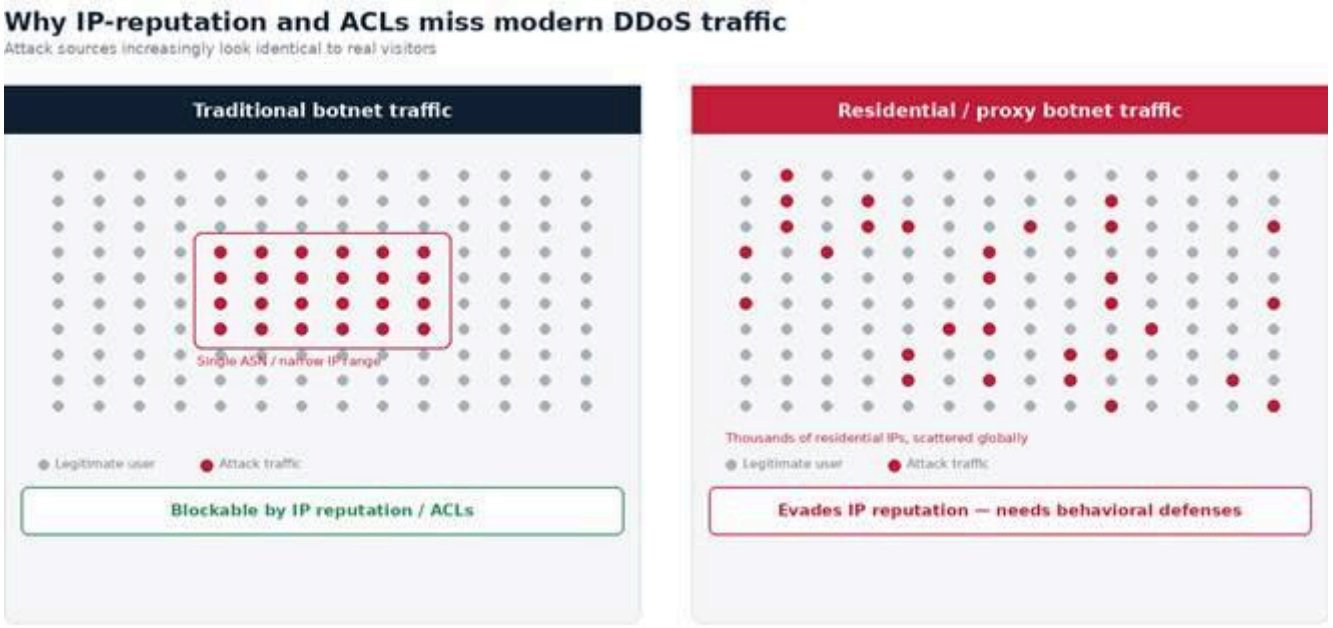
If your organization has predictable high-traffic or high-visibility windows - a product launch, a ticket sale, a seasonal peak, an earnings call, or a major industry event - treat that window as a period of elevated DDoS risk. Confirm your incident response team is staffed and ready before the event, not during it. If it's been a while since you last tested your protection under real attack conditions, a DDoS simulation ahead of your next big moment is the clearest way to know where you stand.

ALSO WORTH KNOWING

Old Routers, New Risk: The AryStinger Botnet

In June, researchers uncovered a new malware campaign, dubbed AryStinger, that has quietly compromised more than 4,300 home and small-office routers around the world - mostly older D-Link and Realtek-based devices with known, unpatched vulnerabilities, some dating back a decade.

Unlike the classic Mirai-style botnets that made headlines in past years, AryStinger isn't currently being used to launch DDoS attacks - researchers describe its purpose today as reconnaissance and traffic-proxying. But it's a useful reminder of a broader shift that matters more directly to how you defend against DDoS: attackers increasingly build and rent access to large pools of residential IP addresses - real home routers and consumer devices - rather than relying on data-center botnets. Traffic from a residential botnet doesn't look like an attack. It looks like thousands of ordinary home users, because in a sense, it is.



Traditional data-center botnets cluster in narrow IP ranges and are easy to block. Residential and proxy botnets - the category AryStinger belongs to - blend in with real users and defeat IP-based blocking.

WHAT THIS MEANS FOR YOU

This is the practical takeaway: if your DDoS defenses still lean heavily on IP reputation lists, geo-blocking, or static ACLs, that approach is losing effectiveness against this category of attack - the traffic simply doesn't have a 'bad neighborhood' to block. Make sure your protection includes layers that don't depend on knowing an IP is malicious in advance: rate-limiting tuned to your real traffic patterns, behavioral and bot-detection capabilities, and application-layer controls that can spot abuse even when it arrives from thousands of distinct, individually clean-looking sources.

FROM RED BUTTON

Stay Ahead of the Threat

Red Button helps organizations understand and validate their DDoS resilience through authorized, real-world attack simulations, technical advisory, and continuous threat intelligence. If either of the stories in this issue raised questions about your own environment - whether it's readiness for a high-visibility event or the strength of your current protection layers against residential-style traffic - your Red Button team is here to help.

“The DDoS threat landscape evolves constantly. Our job is to make sense of it before it becomes your problem.” - Red Button Red Team & Threat Intelligence

If you'd like to discuss how these trends apply to your environment, contacting your technical manager is the best place to start.

DDoS Threat Pulse is produced by Red Button's Red Team & Threat Intelligence function and compiled from publicly available research and vendor reporting. It is intended as general awareness content for Red Button customers and does not constitute a personalized risk assessment of your environment.