RED BUTTON
DDoS Experts

Red Button DDoS Threat Pulse - July 2026

02/08/2026

CONFIDENTIALITY & PROPRIETARY

DDoS Threat Pulse

Your monthly briefing on the DDoS threat landscape

July 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.

A note on this issue: our Threat Intelligence audit tracked 116 possible DDoS-related events across public reporting and hacktivist channels in July. The large majority - 96 - were unverified claims relayed by hacktivist groups on social media, with no independent confirmation that any service was actually affected. Only 15 events were independently confirmed or provider-attributed as DDoS. The stories below focus on the confirmed cases, plus a look at what this month's claim data does and doesn't tell us.

IN THIS ISSUE

- Carpet-bombing DDoS attacks took down internet service providers on two continents in one month- and why the technique is now one of the growing techniques in the threat landscape
- A 36-hour, multi-vector campaign on a Malaysian hosting provider.
- The same piece of shared gaming-voice infrastructure was hit by five confirmed DDoS attacks in a single month - a case study in third-party single points of failure
- Of 116 tracked events in July, only 10 named a hacktivist actor at all - and none of the 20 confirmed DDoS incidents did

Two Continents, Two ISPs: Carpet-Bombing Goes Mainstream

In July, Red Button's Threat Intelligence team tracked confirmed carpet-bombing DDoS attacks against internet service providers on two different continents - a reminder that a technique once considered a niche curiosity is becoming one of the default ways attackers take down infrastructure at scale.

For those of you who are not familiar with this kind of attack, a "Carpet Bombing" is a DDoS technique which targets whole network ranges at the same time instead of targeting only a specific IP address. That keeps the volume hitting each individual host below the threshold most legacy, per-IP DDoS protections are tuned to catch, even though the attack's total volume against the network is just as large. According to Flowtriq's State of DDoS 2026 report, carpet-bombing rose to about 12% of tracked incidents in 2025, up from roughly 4%, growing faster than any other DDoS technique the report tracked.

On July 19, US-based ISP Zeta Broadband published a postmortem confirming a large-scale carpet-bomb DDoS attack that saturated its upstream links, starting around 12:30 Pacific time and knocking out service for its customer base network-wide for roughly 12 hours. A little over a week earlier, Jenny, an internet service provider in southern Africa, spent two days publishing incident updates describing a carpet-bomb DDoS attack that self-reportedly peaked above 1 Tbps and spread across multiple /24 subnets, causing intermittent connectivity and degraded routing for customers.

ISPs face this differently than most enterprises do in the first place: they're both direct targets and targets-by-association for every customer they host, and - unlike enterprises leaning on prefab cloud DDoS protection - they largely have to build, operate, and maintain their own mitigation in-house. Red Button's own research goes into this in more depth in DDoS Attacks Targeting ISPs are Different - Here's How.

WHAT THIS MEANS FOR YOU

Carpet-bombing can hit either side of your infrastructure: an IP range your own organization owns and manages, or the shared address space of an ISP or hosting provider you rely on. Either way, the same question applies - Does DDoS detection work at the subnet level, not just the individual IP or host level? If you manage your own IP range, ask your own security team or DDoS protection vendor whether detection covers your full range, not just individual hosts, and even test it with a dedicated DDoS simulation to approve that. If you rely on an ISP's or hosting provider's address space, ask them the same question about their network. If detection is purely per-IP in either case, a carpet-bombing attack spread across the range could degrade your service even if no single IP was heavily targeted. If you haven't confirmed this for your own environment - and your provider's, if applicable - now is a good time.

When the Host, Not the Site, Is the Target: A 36-Hour Multi-Vector Attack

Between July 5 and 7, Shinjiru, a Malaysian web hosting provider used by thousands of businesses across the region, confirmed on its status page and official LinkedIn that its network had been hit by what it called a "Dynamic Multi-Vector DDoS attack" lasting roughly 36 hours. Rather than one type of flood, the attack combined UDP floods, TCP state-exhaustion, IP carpet-bombing, and direct Layer 3/BGP-routing attacks against multiple ports at once - and, per Shinjiru, the attackers continuously shifted tactics to exploit the timing gaps between each new filter-rule deployment.

Because the attack targeted Shinjiru's network rather than any single customer's website, sites hosted on that network saw intermittent connectivity errors even where their own servers stayed completely healthy the entire time. The problem was never at the site level; it was upstream.

This kind of layered attack isn't an outlier. Red Button's own July analysis of the 2026 DDoS landscape, DDoS Attack Trends in 2026: Scale, Precision, and the Gaps in Between, calls out multi-vector campaigns - combining hyper-volumetric network floods with other techniques to stress multiple layers at once - as the new standard rather than the exception.

WHAT THIS MEANS FOR YOU

If your infrastructure sits on shared hosting, a CDN, or any upstream provider, ask that provider directly what their DDoS protections are, and if they are willing to be tested by Red Button. If your hosting provider does not provide you this information, it can be a red flag and may impact your service availability in the future. In addition, consider using multi-vector scenarios in your future DDoS tests with Red Button, as they may act differently from a single vector scenario.

One Target, Five Attacks: A Recurring Hit on Shared Gaming Infrastructure

Throughout July, Unity's Vivox voice and text communications service - an SDK embedded in a large number of online games - reported five [5] separate confirmed DDoS attacks against its infrastructure on its own status page: July 2, July 3, July 26, July 27, and July 28. Each incident affected the signaling layer used to establish voice and chat connections, with individual outages lasting anywhere from a couple of minutes to just over an hour.

No single incident lasted long. But five confirmed attacks against the same infrastructure provider within one month is a pattern worth noting - particularly because Vivox is shared, third-party infrastructure embedded inside many different games and apps at once. Any game/product relying on it inherits the outage the moment Vivox is hit, regardless of that title's own DDoS protections.

WHAT THIS MEANS FOR YOU

If your product embeds a third-party real-time communication service - voice chat, in-app messaging, live support widgets - that vendor's DDoS resilience is now part of your own resilience posture, and it's largely outside your direct control. Ask embedded-service vendors what DDoS protections they run and how quickly they detect and mitigate, and build a fallback or graceful-degradation path for when that dependency goes down, rather than assuming it never will.

ALSO WORTH KNOWING

When a DDoS Attack Kills Off Video-Game Characters

On July 21, a malicious DDoS attack hit three World of Warcraft Classic Hardcore realms in North America - a game mode where character death is permanent by design. The disruption caused enough players to disconnect mid-fight that a number of Hardcore characters died as a direct result of the attack rather than through ordinary gameplay risk.

Blizzard's response was notable: the company restored the lost characters, an exception to its usual hands-off policy on Hardcore deaths. Blizzard had set this precedent once before, after an earlier DDoS incident affected a well-known streaming guild; leadership said at the time that a DDoS attack is a deliberate act by an external bad actor, which the company treats differently from an ordinary in-game death.

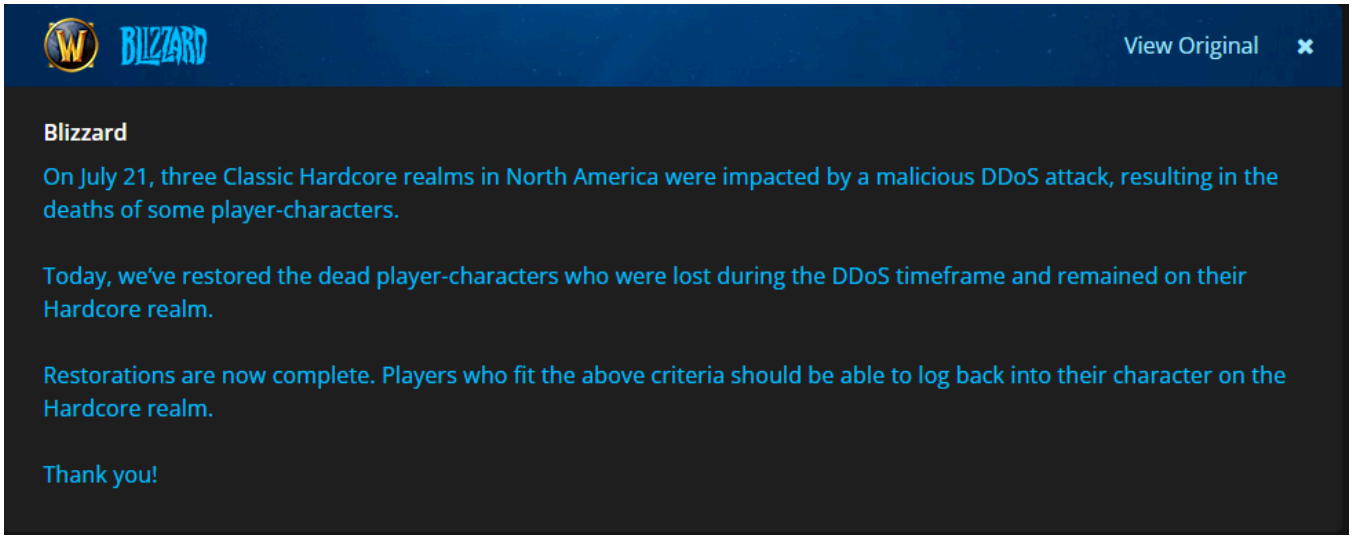

Figure 1.0 - *Blizzard's post-incident announcement*

WHAT THIS MEANS FOR YOU

If you are an organization providing online gaming services, ensure you have the appropriate GRC policies in place to address situations where players lose in-game assets due to an infrastructure outage. This field is generally referred to as "business DDoS playbooks." We recommend that every organization develop one, making it as detailed as possible, to avoid surprises during the next attack. Red Button customers benefit from the expertise of the company's engineers and consultants, who have previously assisted numerous organizations in creating such playbooks.

Who's Behind the Noise: Hacktivist Attribution in July

Looking at all of July's unverified hacktivist claims together - not just the ones naming an actor - a few clear patterns stand out. Local and regional government was by far the most common type of target. Municipal councils, transport authorities, and other public-sector bodies drew more claims than any other category combined, while large private companies were claimed far less often. When private targets did show up, they leaned toward aviation and port/shipping operators rather than banks, retailers, or tech platforms.

Geographically, Europe was the center of gravity. Germany, Spain, Poland, Romania, Ukraine, and France between them accounted for close to half of everything claimed this month, with Israel the largest cluster outside Europe. Activity also built as the month went on rather than staying steady. Claims were relatively quiet in early July, picked up through the middle of the month, and peaked in the final full week, with a short, sharp cluster in one two-day stretch - the busiest moment of the month. This is a phenomenon we have certainly been witnessing in recent months: DDoS attacks tend to occur precisely when legitimate traffic is expected to be at its peak, usually at the beginning or end of the month.

Where a claim did name a group, each one seemed to have its own lane. **NoName057(16)**, a long-running pro-Russian group, stuck to its usual pattern: government and public-infrastructure targets in Poland, consistent with its broader focus on countries seen as supporting Ukraine. **Dark Storm Team**, a pro-Palestinian group, cast a wider net - European municipal networks on one hand, a major consumer gaming platform on the other - more opportunistic than targeted. **313 Team**, a pro-Iran-aligned group, went after Western cloud and productivity platforms, continuing a pattern seen elsewhere this year of the group targeting large, recognizable tech brands rather than smaller organizations. The remaining named claims - one against an Israeli utility, two against Thai targets from lesser-known groups - were one-off and regionally specific rather than part of any broader pattern. Most claims, though, named no group at all. The large majority arrived without any attribution - just a claim of impact, with no name attached.

WHAT THIS MEANS FOR YOU

If your organization is a local or regional government body, July's data suggests you're sitting in the highest-volume target category, regardless of whether any specific group has your name on a list. It's also worth remembering that hacktivist activity tends to build over a month rather than arrive evenly, so an early quiet period isn't a reliable sign it'll stay that way. And since most claims carry no group name at all, treat an anonymous claim about your organization with the same seriousness as a named one - the absence of an attributed actor doesn't tell you anything about whether the claim is genuine.

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 any of the stories in this issue raised questions about your own environment - whether it's how your provider handles carpet-bombing or multi-vector attacks, your exposure to a third-party service outage, or how you'd weigh a hacktivist claim against your own organization - 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.