Delux HOST

TECHNICAL POST-MORTEM

Infrastructure incident & DDoS attack

6 – 23 June 2026

This document is a transparent reconstruction of the events that affected our infrastructure between 6 and 23 June 2026: what happened, where we got it wrong, and what we are doing to make sure the same mistakes don't happen again. It was written to give you a precise account — not a polished press release.

THE ATTACK IN NUMBERS

These are figures that would put pressure on infrastructures far larger than ours. We don't cite them as an excuse — our responsibility remains intact — but as context for what hit us and why some difficult calls had to be made.

>3 Tbps	**~400 Mpps**	**~14 days**	**Carpet**
PEAK VOLUMETRIC ATTACK	PACKETS/SEC, MAIN WAVES	TOTAL EVENT DURATION	ATTACK PATTERN — MANY IPS IN PARALLEL

AT A GLANCE

6 Jun	Cooling system failure on a rack, plus a secondary network hardware fault.
7 – 10 Jun	DDoS carpet bombing begins. ~3.5 h of downtime per day — the worst phase.
11 – 20 Jun	Attacks declining, but recurring network drops. Prolonged disruption for customers on legacy storage.
From 20 Jun	Service stable. RETN activation as a backup backbone in the coming days.
Already done	One extra week of renewal automatically credited to all active services.
Coming next	Dedicated email on SLA and compensation by Sunday 28 June.

01 Timeline of events

The incident went through four distinct phases, each with different characteristics and impact on services.

6 June

Cooling system failure

A fault in the cooling system of one rack triggered thermal protection. In the hours that followed, a secondary hardware failure on a network component amplified the impact, requiring manual recovery interventions.

7 – 10 June

Prolonged downtime and start of the DDoS attack

While we were still stabilising from the hardware fault, a DDoS carpet bombing campaign began. There were effective and prolonged outages — on the order of **~3.5 hours per day**, distributed across the attack waves. This is when the impact was worst.

11 – 20 June

Prolonged instability and disruption on legacy storage

Attacks still active but progressively declining. Recurring network drops which, for customers on legacy storage, caused prolonged disruption even after the attack subsided — requiring a manual VPS reboot for full recovery. For these customers the perceived disruption was much longer than the actual attack window.

From 20 June

Stabilisation — with caution

Service back to stable, due both to the natural decline of attacks and — above all — to mitigation filters custom-built for us by our upstream providers. We are keeping enhanced monitoring in place because new waves cannot be ruled out. In the coming days we will activate RETN, a tier-1 European upstream, as an additional backup backbone with extra mitigation capacity, thanks to backbone.direct (AS50917).

02 Root cause analysis

2.1 — INITIAL INFRASTRUCTURE FAILURE

The 6 June event was triggered by a fault in one of the rack cooling systems. Thermal protection acted as designed, but the concurrent failure of a network hardware component generated a cascade effect that required manual intervention. The affected hardware has been replaced; environmental and thermal monitoring across the racks has been extended to anticipate similar conditions earlier.

2.2 — THE DDOS CARPET BOMBING CAMPAIGN

From 7 June we registered recurring waves of hostile traffic in carpet bombing mode: instead of concentrating on a single IP, the attack distributed its volume across dozens of destinations within our IP range simultaneously. This pattern is particularly hard to mitigate because it bypasses many traditional single-target defences. Calibrating upstream filters took several iterations — loose filters let the attack through, tight filters blocked legitimate traffic. The turning point came with custom filters built by our upstream providers specifically around the observed patterns.

2.3 — LEGACY STORAGE SYSTEMS

A share of our customers is still hosted on legacy storage systems. This isn't twenty-year-old hardware, but a class of systems that shows a specific behaviour under prolonged network-drop conditions: even after connectivity is restored, some VPS require a manual reboot to return to full operation. Migration to newer storage was already planned independently of this event; it is now being heavily accelerated, because the incident made clear it should have been completed sooner.

03 Where we got it wrong

This is the section that matters most to us, because the only serious way to deal with something like this is to call things by their name. We take ownership of our mistakes — there are points where we promised more than we could deliver in a situation like this.

DDoS mitigation was too slow

Our initial response to the attack wasn't as fast as it should have been. Switching to or integrating upstreams with higher mitigation capacity takes real technical time — it isn't something you complete in 48 hours — but even within those constraints, some decisions could have been made earlier and better.

Upstream filters were too aggressive for days

To stop the attack we accepted very strict upstream filters for several days. They protected the infrastructure but also blocked legitimate traffic, especially from certain geographies. It was a conscious trade-off, and one that has to be acknowledged as such.

Legacy storage not yet migrated

We knew that generation of storage needed replacing. The migration was planned, but not prioritised enough. This event showed the priority should have been raised earlier — we've raised it now, but it should have happened before.

Slow communication in the early days

In the first days of the incident our communication wasn't as structured as it should have been. Many of you were left in the dark about what was going on, and that is not acceptable.

04 What we're doing

Actions completed, in progress and planned. By the end of August 2026 we will publish a verification update documenting what we actually implemented of what we promised here — we want our commitments to be verifiable, not just stated.

STATUS	ACTION
COMPLETED	Replacement of the hardware involved in the 6 June failure
COMPLETED	Extended environmental and thermal monitoring across racks
COMPLETED	Activation of custom DDoS filters with our upstream providers
IN PROGRESS	Activation of RETN, via backbone.direct (AS50917), as tier-1 backup (this week)
IN PROGRESS	Acceleration of the migration away from legacy storage systems
IN PROGRESS	Internal review of incident response procedures
PLANNED	Dedicated communication on compensation and SLA (by 28 June)
PLANNED	Public verification update by the end of August 2026

Cooperation with law enforcement

The DDoS attack is a criminal offence under Italian and EU law. We have filed a formal complaint with the Italian Postal and Communications Police (Polizia Postale) and reported the incident to CSIRT Italia (the National Cybersecurity Agency's incident response team), sharing the technical data collected during the event to help identify those responsible.

With thanks to Backbone.Direct

Getting through this incident owed a great deal to the support of Backbone.Direct (AS50917). Their team worked closely with us on upstream mitigation and on the custom filters that finally brought the carpet bombing under control, and they are the partner bringing RETN online as our additional backup backbone. We're grateful for their responsiveness throughout the most difficult phases of the event.

05 Support & contacts

If you're still experiencing problems, contact us right away. The team is on enhanced monitoring duty and is responding with priority to anything related to this incident.

IF YOUR VPS ISN'T RESPONDING CORRECTLY

1. Run a reboot from the control panel — not a soft reboot from inside the VPS.
2. If you still can't reach the VPS, try connecting via VPN to rule out issues caused by upstream filters towards your geographic area.
3. If the problem persists, write to support@deluxhost.net — our team will intervene directly on the hypervisor.

SUPPORT EMAIL	STATUS PAGE
support@deluxhost.net	**status.deluxhost.net**