RED BUTTON
DDoS Experts

Red Button
DDoS Threat Pulse

August 2026

In this Issue

- Norway's national login system went down twice in one month, and took banks with it that nobody attacked
- 600 Gbps landed on a Swiss hosting company, and the customer everyone noticed was probably not the target
- An attack on an email provider ended in an hour. The damage it set off ran for another four days.
- Small Polish internet providers were offered protection for 2,000 złoty, payable in shop-bought gift vouchers
- New research shows how to make a CDN produce the attack traffic that hits the origin behind it

About the DDoS Threat Pulse

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.

When the Login Goes Down, So Does Everything Behind It

Norway runs most of its public services behind a single sign-in called ID-porten. It is how people reach the tax office, the health portal and their local council, and it is operated by Digdir, the government agency responsible for the country's shared digital infrastructure. At 03:38 on the morning of 24 August, someone started flooding it.

The attack ran for about 63 hours.. Digdir called it the biggest it has ever dealt with, 2-3 times the size of the last one. Twelve shared national services were named as hit or affected: the login system itself, the government's secure digital post service, the service that lets agencies exchange data with each other automatically, the business reporting portal, and the electronic signing service among them. Everything was back to normal by the afternoon of the 27th.

This was the third time in a short stretch. One attack in late June was followed by another on 3 August that kept the login system down for more than a day. That one also reached the national system that carries electronic prescriptions from doctors to pharmacies, and at least one national pharmacy chain confirmed it was affected.

The interesting part is who else went down. Four Norwegian banks spent the 24th telling customers that transfers, payments and account balances were misbehaving in their online and mobile banking. None of them had been attacked. They shared an IT supplier, and that

supplier's services depended on the login system that was under attack. Its communications chief said as much publicly: “The flood was aimed at the government gateway, and their own services broke as a knock-on effect. Nobody's DDoS protection failed. The dependency chain just happened to run through something that was being hit”.

A pro-Russian group calling itself Server Killers claimed responsibility on Telegram two days in, tying it to Norway's renewed support for Ukraine. Digdir has not confirmed that, and neither has Norway's national security authority or its police security service. Digdir found no sign that anything was breached or that personal data went anywhere, and says it received no ransom demand.

> **WHAT THIS MEANS FOR YOU**
>
> Somewhere in front of your service there is probably a login you don't own. A national eID, a federated identity provider, a payment authentication step, a shared SSO. Whatever it is, your uptime cannot be better than its uptime, and a test that only points at your own infrastructure will never show you that. So the question to put to your team this month is a blunt one: **what can break us while our own servers are completely healthy?**

600 Gbps Landed on the Provider, Not on the Customer

On the evening of 11 August, Threema, a Swiss encrypted messaging app, dropped offline for roughly four hours. Threema was the name people noticed. By its own account it may not have been the point: the company said it isn't clear whether it was the primary target or one of several.

The numbers came from Nine, the Swiss company that hosts it, in a postmortem covered by the Swiss IT press. The attackers used UDP amplification. At its peak the flood hit 500-600 Gbps, which Nine described as several times its own uplink capacity. Nine's website went down too, along with the platform its customers' applications run on, the control panel they would use to manage them, and its support ticketing system. For a while, affected customers lost their service, the tools to fix it, and part of their route to ask for help, all at once.

Two things stand out. Nine's traffic monitoring didn't cover every network it runs, and the first wave landed on one of the gaps, so it had to be handled by hand. That cost about 90 minutes. And at 600 Gbps the practical answer was blackholing upstream: the provider above you throws away everything addressed to the IP under attack. It saves the network and everyone else on it. It also throws away your real customers. Anyone running Threema on their own servers rather than the hosted service stayed up throughout, and extra filtering further upstream was switched on two days later.

Threema noted that keeping an attack going and adapting it like this takes real money and real technical depth, “as may be the case with state actors”. It did not attribute the attack to anyone, and neither did Nine.

WHAT THIS MEANS FOR YOU

Your provider can answer two questions in about five minutes, and both are useful. How much uplink capacity does the network your service sits on actually have? And at what point do they stop filtering and start blackholing? Blackholing is a reasonable tool, but it is a decision to drop your traffic to protect everybody else's, so you want to know where that line sits and who gets to draw it. A third question is less obvious and was the expensive one here: does their monitoring cover every part of their network, or only the busy parts? The gap cost the first 90 minutes of this incident, not the size of the flood. If a provider won't answer, or won't be tested, that tells you something on its own.

The Attack Ended in an Hour. The Damage Ran for Four Days.

At 15:36 on 13 August, Runbox, a Norwegian email provider, saw its services start failing. An hour later the company had worked out it was a DDoS attack. So far, a short and fairly ordinary incident.

Then it got strange. The flood had left the mail servers with a big backlog, and clearing a backlog means looking up where every one of those messages is supposed to go. Runbox's servers started firing DNS queries at the rest of the internet in enormous volume. Some of the services on the receiving end decided that looked like abuse and blocked them. From that point Runbox couldn't reliably deliver mail, couldn't validate mail settings for the domains it hosts, and couldn't set up new customer domains at all. The incident was formally closed on the morning of the 14th. The delivery problems carried on until a workaround went in on the 17th.

The flood was a first-order problem and it lasted about an hour. The second-order problem was that Runbox's own recovery made it look, from the outside, like the bad guy. That is not a scenario most DDoS planning covers. The usual question is whether you can survive the traffic. This one is different: **what does your recovery plan look like?**

WHAT THIS MEANS FOR YOU

Most incident plans stop at the moment service comes back. This one is an argument for reading a bit further down the page. Two things help. Check whether anything rate-limits your recovery paths, because usually nothing does. And give the recovery phase a named owner in your playbook, so it isn't the bit everyone assumes someone else is watching. Restoration is not resolution.

Two Thousand Złoty, Payable in Gift Vouchers

All summer, small internet providers across Poland were being knocked offline. A Polish cybersecurity outlet counted sixteen of them that had publicly reported problems between 1 June and 6 August. None were large companies. People in the industry told a trade title the real number was several dozen.

What makes this one memorable is the sales pitch. Operators got an email explaining that an attack on their network had been detected, and offering a "Blacklist" service that would keep them safe. The price was 2,000 złoty, about 470 euro. Payment was to be made in prepaid vouchers, the sort of top-up card you buy at a corner shop, in 100 and 200 złoty denominations, with a photo of the receipt sent back so the code was readable. It is an old-fashioned protection racket, priced for a small business, collected in a way that leaves no trail and requires no bank.

The attacks behind it were not trivial. One operator measured around 260 Gbps and more than 80 million packets a second. Another described damage to part of its network and at least a hundred customers who needed an engineer to physically visit. For a provider whose ports run at 1 Gbps, though, it doesn't take 260 Gbps to cause a bad day. Roughly 1 Gbps will do it. Nobody has been publicly confirmed as having paid, and no arrests have been announced.

WHAT THIS MEANS FOR YOU

Ransom DDoS is priced against your accounts, not the attacker's ambition. The demand is meant to look cheaper than the outage, which is exactly why it gets paid quietly and why paying marks you as somebody who pays. Two things are useful before that email arrives rather than after. One is a decision, made by management and written down, about whether your organization pays at all, so it isn't taken at two in the morning by whoever happens to be on shift. The other is knowing the answer to what the demand is really asking, which is whether you can take the hit if you say no. We have worked incidents where the first attack arrived the same day as the threat, so there isn't much time to find out. If you're a smaller operator without your own scrubbing capacity, this is the scenario to test first.

Turning a CDN Into the Attacker

A CDN sits in front of your website, takes the traffic, and passes on what it needs to your own servers behind it. Almost all of the big ones now accept the newest version of the web protocol, HTTP/3, from visitors, then translate it into an older version when they talk to your servers. In August, academics from the National University of Singapore, Fuzhou University, the University of Sheffield and Johns Hopkins showed that the translation step can be turned into a weapon. They call it CDN Tsunami.

The first trick abuses header compression. HTTP/3 lets a browser send a tiny shorthand reference instead of a full set of headers, and the CDN expands it back out before passing it on. Send the shorthand, and the CDN generates the full-size request against your origin for you. Across the six major CDNs the researchers tested, that multiplied the attacker's traffic by somewhere between 36 and 66 times, and on three of them it went as high as about 350. The attacker's own connection stayed under half a megabit per second. The second trick is quieter: it uses HTTP/3's ability to run many requests down one connection so that each one opens a separate, slow connection to your origin, until the origin runs out. Five of the six were vulnerable to that. The one that wasn't behaves differently by design, holding the whole request before it opens anything at the back.

Taking a standard list of the internet's million busiest domains, the researchers found 42,330 subdomains on those six CDNs that answer HTTP/3 and could be exposed. No CVEs have been issued, nobody has seen this used in a real attack, and two of the six vendors have already shipped fixes. So this is a story about what's coming rather than what happened. It is on our list anyway, because the traffic it produces reaches your servers from your own CDN's addresses, which is precisely the traffic almost every origin is configured to trust. The paper names which CDN behaved which way, if you want to check yours.

WHAT THIS MEANS FOR YOU

There is one assumption here that most architectures make and nobody writes down: traffic arriving from our CDN is safe, because it came from our CDN. The rule that encodes it, allow the CDN's ranges and block everything else, is correct and you should keep it. It just means an attack that gets the CDN to do the work shows up pre-approved. Nothing needs changing this week, since nobody is doing this yet. What's useful is knowing two things before somebody does: whether anything behind that allowlist limits request rates or connection counts on its own, and what your CDN vendor has said about this research. If the whole design rests on one CDN getting it right, that's a dependency, and dependencies are testable.

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 anything in this issue raised a question about your own environment - the shared services sitting in front of your login, how your provider behaves when filtering turns into blackholing, or what your systems do to everyone else while they recover - 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

Confidentiality & Proprietary