RED BUTTON
DDoS Experts



Red Button
DDoS Threat Pulse

October 2026

All rights reserved.This document is protected by copyright and any distribution, reproduction, copying recompilation is strictly prohibited without the prior written consent of Red Button. No part of this document may be reproduced in any form or by any means without the prior written authorization or Red Button. This document and information is intended solely for the internal use of authorized Red Buttond Ltd. customers, for the limited purposes set forth herein. While every precaution has been taken in the preparation of this document, Red Button assumes no responsibility for errors or ommisions.

In this Issue

- Thirty-Two Hours Without North Korea's Websites
- Rented Firepower Against a Whole Government
- Month Three for Poland's Small ISPs, and the Government Steps In
- When the Service Everyone Leans On Goes Down
- Attacks Timed to the Moment That Counts
- The Botnets Are Growing Back
- Stay Ahead of the Threat

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.

© All rights reserved. Red Button

Thirty-Two Hours Without North Korea's Websites

At 02:01 UTC on Tuesday 20 October, a flood of traffic started hitting North Korea's small corner of the internet. For the next 32 hours, more than 40 of the country's state websites went down and came back again and again. The list included the foreign ministry, the state news agency KCNA, the ruling party's newspaper and the national airline. According to South Korean broadcaster SBS, they were stable again only around seven in the evening, local time, on 21 October.

Doug Madory of Kentik, a US company that monitors internet traffic, was watching. “This traffic all started at the same time and is coming from Vietnam and Venezuela,” he told Reuters. “That's definitely a DDoS attack.” Kentik saw only part of the traffic, and where it came from says nothing about who sent it. Nobody has claimed the attack. Early South Korean reports had suggested unstable power, but Kentik's traffic data pointed to an attack. Reuters also found no link to the PHP flaw that was causing panic elsewhere that week, which we cover below.

The detail that matters most for everyone else is a technical one. North Korea's whole internet presence sits on a handful of address blocks. One of them holds the name servers for the .kp domain, the machines that turn a site's name into an address. That block went down repeatedly during the attack. So even a website that was still running could not be found, because the directory that pointed to it was out. KCNA alone was offline for 19 of the first 24 hours.

Few organizations are as exposed as a whole country squeezed onto a few address blocks. But plenty have the same weakness at a smaller scale: the website, the DNS and the mail all sitting on one network, behind one upstream provider. When that network is flooded, there is no part of the service left to fall back on.

> **WHAT THIS MEANS FOR YOU**
>
> Look up where your own name servers live. If they sit on the same network as the websites they point to, one flood takes out both, and your status page probably goes with them. Spreading authoritative DNS across at least two unrelated providers is cheap and rarely painful. The harder part is the inventory: which address blocks carry your public services, and which of them share an upstream link. That is the map an attacker draws first, so it helps to have drawn it yourself.

© All rights reserved. Red Button

RED BUTTON DDoS Experts

Rented Firepower Against a Whole Government

At around ten in the evening on 13 October, attacks began on more than 100 of Azerbaijan's state domains. The government's cybersecurity service said that a foreign hacker group was behind it and that several agencies' websites were disrupted. The attacks ran until 15 October. Government bodies, media organizations and Azerbaijan's embassies abroad were all hit.

The investigation turned up the more interesting part. The national CERT, the country's computer emergency response team, found that the attackers had used a commercial DDoS service called Litterbox, also known as Catbox. It is sold through Telegram channels and paid for in cryptocurrency. It offers several kinds of flood, and buyers can choose which countries the attacking bots sit in. That makes blocking traffic by country far less useful. An hour before the attacks were detected, a group calling itself 313 Team had announced the operation on Telegram, citing restrictions on headscarves in schools. It said it had used more than 2.5 Tbps and taken 1,825 government websites offline. The authorities have confirmed neither figure, and say the impact was contained.

Azerbaijan was not alone. In Bavaria, the district administration in Cham lost email, phones and internet for several hours on 8 October. Because the district office also runs the network for the municipalities around it, they had to work with restrictions too. The requests came from about 50 countries. The same day, Italy's foreign ministry said its website had been under attack since that morning. It said the attack was “effectively mitigated” without any disruption. Italian press reports blamed NoName057(16), a long-running pro-Russian hacktivist group. The ministry itself attributed it to no one.

Litterbox is the part to remember. Last month we wrote that a one-off attack can be bought for $30. Azerbaijan shows the same DDoS-for-hire market being turned on a national government. Whoever was behind it did not need a botnet of their own. They only needed to pay.

WHAT THIS MEANS FOR YOU

A service that lets the buyer pick the attack's apparent country makes geo-blocking a weak first line. Plenty of public-sector plans still start with “block traffic from abroad”. That move can still help, but it won't save you on its own, and it may be blocking your own citizens overseas, the very people an embassy site exists to serve. The Cham case adds a second point. When one office runs the network for others, its outage becomes theirs. If you are that shared hub, the people downstream need to know, and so does your incident plan.

© All rights reserved. Red Button

Month Three for Poland's Small ISPs, and the Government Steps In

In August we wrote about small Polish internet providers being knocked offline and offered "protection" for 2,000 złoty in shop-bought vouchers. In October the attacks spread. Fiberlink in the south switched to backup links around 7 October. Oxynet in Jarosław fought an "unusually large wave" on 10-11 October, and ProIP, near Warsaw, was hit again two weeks after its last attack.

The biggest so far is JMDI, one of Warsaw's largest local operators. It warned customers that an attack on its network had been announced, and on about 21 October it began. JMDI described hundreds of gigabits per second at the peak, and hundreds of millions of packets per second. The flood "jumps between successive addresses", so the outages popped up in scattered spots. That pattern is typical of carpet-bombing. JMDI temporarily limited traffic from foreign networks and warned that its own customer hotline might go down. On 27 October it was still refusing to "raise the victory flag".

This month the state got involved. On 13 October UKE, Poland's telecom regulator, asked operators to report every DDoS incident. On 26 October the Ministry of Digital Affairs published updated recommendations for internet providers. They read like a short course in surviving this kind of attack. Keep a backup link from a different provider with its own addressing, and be able to switch in minutes. Keep customer communications off the network under attack. Have a scrubbing contract, and test the diversion. And report attacks even when you beat them. No arrests have been reported.

Poland's providers are not alone. In St Petersburg, the home internet provider SkyNet said it had been under DDoS since 6 October, and a pro-Ukrainian group called BO Team claimed it. Its neighbor PAKT reported attacks on 17 and 26 October. Different country, different attackers, same target: the local provider.

> **WHAT THIS MEANS FOR YOU**
>
> The Polish ministry's list was written for internet providers, but most of it applies to anyone whose business depends on staying online. Read it as a self-test. Could you move your traffic to a second provider in minutes, not hours? Would your customers hear from you if your own network were the thing under attack? Has the diversion to your scrubbing service been exercised this year, or only signed? And when you fend off an attack quietly, does anyone outside the team ever hear about it? Reporting repelled attacks is how a regulator sees a campaign before it reaches the next victim.

© All rights reserved. Red Button

When the Service Everyone Leans On Goes Down

On the afternoon of 8 October, Canonical, the company behind the Ubuntu version of Linux, posted that its websites were “under a sustained distributed denial of service attack”. The main sites, the Ubuntu blog, the developer site and the security notices went offline. So did the Ubuntu Security API, which tools use to check which fixes apply to a system. According to OMG! Ubuntu, a long-running Ubuntu news site, the main websites were down for about four hours. The package servers that deliver the updates themselves stayed up. Canonical declared everything restored on 14 October. Nobody claimed the attack.

It was Canonical's second big attack this year. The first started on 30 April and ran into May. That time it took down much more, including the services some users needed to install updates. 313 Team, the same group that claimed the attack on Azerbaijan this month, claimed that one too. Canonical has never confirmed the claim.

The month had more of these. On 24 October Lolipop, a large Japanese shared-hosting service, reported that a DDoS on its DNS servers had made name lookups unreliable for about an hour. During that hour, customers' websites and email were hard to reach. In Paris, the cloud platform Clever Cloud logged two DDoS incidents, on 15 and 21 October. The second hit a load balancer that several customers share.

Two patches from this month fit the same pattern. ISC, which maintains BIND, the most widely used DNS server software, fixed a flaw on 21 October that lets crafted DNS messages exhaust a server's CPU and memory. There is no fix for the 9.18 branch, so users of that version have to upgrade. HAProxy, a load balancer found in front of a great many websites, fixed two bugs on 27 October. A handful of malformed requests can tie up all of its processing threads.

WHAT THIS MEANS FOR YOU

The question here is not whether your own servers can take a flood. It is which shared services sit between you and your customers, and which ones sit between you and your fixes. DNS, a hosting provider's shared load balancer, a vendor's security feed: each is someone else's attack surface that becomes your outage. Two habits help. Know which of your services ride on shared layers, and ask those providers how they isolate one customer's attack from the rest. And don't let patching depend on a single live connection to a vendor's website. A local mirror or cached feed means the next attack on a vendor doesn't stall your updates.

© All rights reserved. Red Button

Attacks Timed to the Moment That Counts

At 08:00 on 9 October, France's center-left opened online voting in its joint primary to choose a candidate for the 2027 presidential election. From that moment the platform was hit by what the organizers called "a massive, fake surge of connections". Bots pushed the number of simultaneous connections to the maximum the system could hold. The organizers said the platform never stopped working and that no votes were compromised. But it slowed the vote down. By seven that evening, only about 20,000 of some 140,000 registered voters had managed to vote.

The organizers extended voting until Sunday evening, and the three parties went to the courts. The Paris prosecutor's cybercrime section opened an investigation, and ANSSI, France's national cybersecurity agency, was brought in at the prime minister's request. Nobody has claimed it.

Elections are the obvious case, but the logic works anywhere a deadline matters. In Denmark, an online auction house was selling off the stock of a bankrupt furniture brand when a DDoS hit in the final phase of the auction. The house had to stop the sale and cancel every bid placed. And on 11 October, one of the month's biggest video game launches lost part of its online play. Five days after release, the studio confirmed that disconnects and login problems were down to DDoS attacks on its online services.

None of these attacks needed to last long or be very big. They only needed to land on the one moment when being unavailable costs the most: the opening of a vote, the last minutes of an auction, launch week. Anyone who wants to cause damage can read a calendar.

WHAT THIS MEANS FOR YOU

Most organizations have a few moments a year when an hour offline costs more than a week at any other time. A launch, a sale's closing minutes, a filing deadline, results day. Name yours, and plan protection around them, with the same care you give the rest of the year. Two points from this month. The French attack did not knock anything over. It filled the connection slots, so size for simultaneous sessions as well as bandwidth, and know how you will tell bots from people at the front door. And decide in advance who can extend a deadline or rerun an auction. That decision, made calmly beforehand, is what keeps an attack from deciding the outcome.

© All rights reserved. Red Button

The Botnets Are Growing Back

This spring, police and industry took apart some of the biggest DDoS botnets ever seen, and in May the alleged operator of one of them was arrested. The effect is already wearing off. Qrator Labs, a DDoS-protection company, reported that the largest botnet it fought in the third quarter had 3.56 million devices. That is about 70% more than the second quarter's largest, although still well below the record 13.5 million it saw at the start of the year. The longest attack Qrator saw lasted 200 hours, more than eight days, against a bank. Financial services drew almost a third of all attacks. “Takedowns can seriously disrupt even the largest botnets,” said its CTO, “but their effect is temporary.”

The botnets are also getting smarter about what they send. Corero, another protection company, took apart 3,322 samples of the malware that turns routers, cameras and servers into attack bots. Eight in ten could launch at least two kinds of attack, and some up to eleven. More than 800 samples pretend to be ordinary web browsers. Many add random strings to the web addresses they request, so a CDN cannot answer from its cache and every request goes through to the server behind it. That is why the origin server matters as much as the edge. One in five samples carries code aimed at a specific hosting provider's protection.

And on 21 October the hunt for new bots got easier. PHP, the language behind a large share of the world's websites, patched two flaws that let anyone run code on a vulnerable server with a crafted request. Within hours, exploit attempts were pouring in. Sophos, a security company, saw attackers try to install a Mirai-based DDoS bot on the servers they targeted. Censys, which scans the internet, counted more than 34 million PHP services that might be vulnerable. Many run versions too old to get a fix at all. The US cybersecurity agency added both flaws to its list of exploited vulnerabilities on 26 October.

The flaw caused its own outages too. On 22 October, government departments, hospitals, banks and broadcasters in several countries took their websites offline as a precaution while they patched. For a day, fear of the bug kept more sites offline than any attack on it had.

> **WHAT THIS MEANS FOR YOU**
>
> Every unpatched server is a potential bot, and this month the botnets came shopping. If you run PHP, the first job is the obvious one. The second is to check what your servers send as well as what they receive. A sudden stream of outbound traffic from a web server is a sign it has been recruited. If you rely on a CDN, look at what reaches the origin when every request carries a random query string. And if you take a service offline as a precaution, treat it like an outage: decide in advance who makes that call and what customers are told.

© All rights reserved. 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 anything in this issue raised a question about your own environment - where your DNS really lives, how quickly you could move to a second provider, or what happens to your service at the one moment it matters most - 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

© All rights reserved. Red Button



Confidentiality & Proprietary

This document contains confidential and proprietary information of Red Button Ltd. ("Red Button") and may not be disclosed outside your organization, transmitted, duplicated, or used in whole or in part for any purpose other than its intended purpose. Any use or disclosure, in whole or in part, of this information without explicit written permission of Red Button is prohibited. Red Button makes no warranty that the information contained in this document is complete or error-free.