whalebone

Peacemaker · Threat Landscape Q3 2026

United Kingdom

758,715,537

threats blocked on Whalebone-protected networks in the United Kingdom in Q3 2026.

That is about 8.4 million blocked requests on British networks every day, and 25% of the 3.1 billion threats Whalebone stopped across six European markets in the quarter. Every one of them was a device inside an ISP's network reaching for a malicious domain.

Malware
79%
Infected devices contacting command, update, and payload servers in the background.

Blacklist
12%
Domains on Whalebone's confirmed-malicious lists, blocked outright.

Phishing
7%
Fake login pages and scam messages that reach the user directly.

Other
2%
Command-and-control traffic, compromised domains, spam, and coinminers.

Inside

What British networks blocked, which global threats reached the United Kingdom, and the fake Lloyds Bank login page built to trap British customers this quarter.

Source: Whalebone threat intelligence, DNS requests blocked on customer networks in the United Kingdom, Q3 2026 (UTC). Shares are of all blocked threats in the market and are rounded to whole percent.

whalebone

Malware is 79% of everything British networks blocked

Malware works in the background: infected devices contact their servers automatically and repeatedly, and every contact is a DNS request. That is why it outnumbers the phishing people actually notice.

What was blocked

Share of all blocked threats in the United Kingdom by type. Other covers compromised, spam, and coinminer domains.



Global threats seen in United Kingdom

Three malicious domains were blocked in every market Whalebone monitors across Europe. In Q3 2026, Whalebone blocked 25,418,660 requests to these three domains coming from devices on British networks.

Domain	United Kingdom	All markets
newsboydurance[.]cfd Redirects, pop-up ads, rogue extensions	14,104,676	73,868,438
adexchangerapid[.]com Adware-associated domain	8,998,787	55,828,407
pool[.]supportxmr[.]com Mining pool used by coinminers	2,315,197	17,442,067

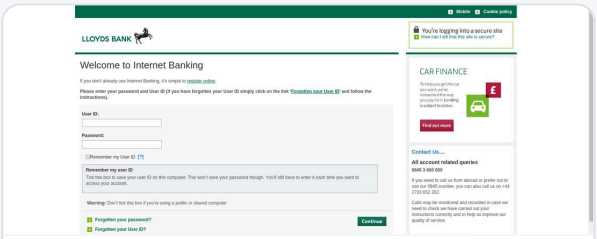
Local threat of the quarter

A fake Lloyds Bank login page targeting British customers

This phishing site targets UK consumers by closely replicating the Lloyds Bank Internet Banking login page. It mimics authentic Lloyds branding to persuade victims to enter their User ID and password.

Whalebone blocks the DNS request before the page loads. The customer never reaches the site.

Domain, defanged for safety: `benetekcorp[.]com`



Screenshot of the site, captured by Whalebone threat intelligence

Period: Q3 2026, 90 days (UTC). Counted: DNS requests to domains that Whalebone threat intelligence classifies as malware, phishing, blacklist, C&C, compromised, spam, or coinminer. Domains blocked by customers' own policies are not counted. Whalebone blocks a domain when its threat score reaches the blocking threshold (80 on average); customers can tune it, so counts reflect each network's settings as well as the threats it saw.

Start today with the first step. Request a free trial on our website or contact us directly.

peacemaker@whalebone.io

whalebone.io/peacemaker-profit

Whalebone Peacemaker Profit

Turn DNS security into revenue

Peacemaker Profit lets British ISPs sell network-level DNS security to households and businesses as a paid, white-label add-on. Nothing to install on end devices, with your own pricing and bundles.

+5%	40%	300+
ARPU boost	Trial-to-paid conversion	ISPs run Peacemaker