whalebone

Peacemaker · Threat Landscape Q3 2026

Germany

1,103,410,265

threats blocked on Whalebone-protected networks in Germany in Q3 2026.

That is about 12.3 million blocked requests on German networks every day, and 36% 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
56%
Infected devices contacting command, update, and payload servers in the background.

Blacklist
30%
Domains on Whalebone's confirmed-malicious lists, blocked outright.

Phishing
12%
Fake login pages and scam messages that reach the user directly.

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

Inside

What German networks blocked, which global threats reached Germany, and the fake local news sites built to trap German readers this quarter.

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

Malware is 56% of everything German 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 Germany by type. Other covers compromised, spam, and coinminer domains.



Global threats seen in Germany

Three malicious domains were blocked in every market Whalebone monitors across Europe. In Q3 2026, Whalebone blocked 43,370,235 requests to these three domains coming from devices on German networks.

Domain	Germany	All markets
newsboydurance[.]cfd Redirects, pop-up ads, rogue extensions	25,493,277	73,868,438
adexchangerapid[.]com Adware-associated domain	16,460,044	55,828,407
pool[.]supportxmr[.]com Mining pool used by coinminers	1,416,914	17,442,067

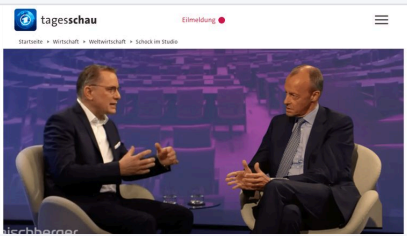
Local threat of the quarter

Fake local news sites targeting German readers

This domain was part of a coordinated cluster of short-lived sites that impersonated local German news media. The cluster delivered social engineering and malware campaigns, trapping both corporate and private users through deceptive browser prompts. Sites like it are rotated quickly, so new look-alikes keep appearing.

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

Domain, defanged for safety: `medienjournal24[.]click`



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 German 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% ARPU boost

40% Trial-to-paid conversion

300+ ISPs run Peacemaker