whalebone

Peacemaker · Threat Landscape Q3 2026

Poland

235,438,995

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

That is about 2.6 million blocked requests on Polish networks every day, and 8% 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
68%
Infected devices contacting command, update, and payload servers in the background.

Blacklist
22%
Domains on Whalebone's confirmed-malicious lists, blocked outright.

Phishing
8%
Fake login pages and scam messages that reach the user directly.

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

Inside

What Polish networks blocked, which global threats reached Poland, and the fake OCHNIK outlet built to trap Polish shoppers this quarter.

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

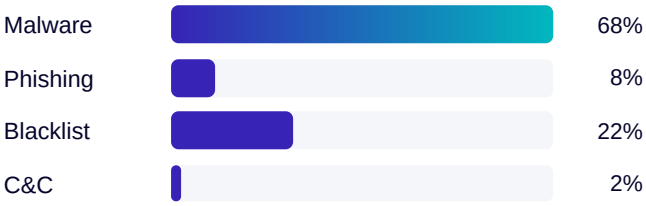
whalebone

Malware is 68% of everything Polish 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 Poland by type. Other covers compromised, spam, and coinminer domains.



Global threats seen in Poland

Three malicious domains were blocked in every market Whalebone monitors across Europe. In Q3 2026, Whalebone blocked 13,493,032 requests to these three domains coming from devices on Polish networks.

Domain	Poland	All markets
newsboydurance[.]cfd Redirects, pop-up ads, rogue extensions	3,626,791	73,868,438
adexchangerapid[.]com Adware-associated domain	1,907,571	55,828,407
pool[.]supportxmr[.]com Mining pool used by coinminers	7,958,670	17,442,067

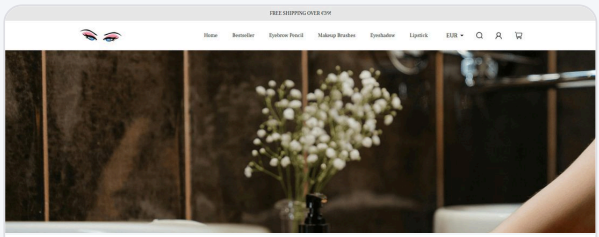
Local threat of the quarter

A fake OCHNIK outlet targeting Polish shoppers

This domain is a confirmed malicious clone of the official outlet of the Polish leather and fashion brand OCHNIK. It is part of a widespread “scam store” network that collects payment details and never ships goods.

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

Domain, defanged for safety: `ochnikoutlet[.]sbs`



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 Polish 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