1) Citation: StevenBlack. (2025). hosts — Unified hosts file with base extensions. GitHub. https://github.com/StevenBlack/hosts

Project Type: Utility Script / Threat-Filtering List

Synopsis:

This repository aggregates and consolidates multiple curated hosts files into a unified hosts file for blocking ads, trackers, malware, and malicious domains. It includes variants and extensions (adware, malware, social media, etc.), scripts to generate and update hosts files, and usage instructions for different platforms. It’s valuable for ransomware defense research because blocking known malicious domains reduces exposure to phishing, and payload infrastructure. Limitations: it’s a preventive list, requires periodic updates, and may produce false positives for some domains.

Dependence/requirements: OS level hosts file access or a hosts manager tool. Project stats: ~29.1k stars, ~2.4k forks, last updated Oct 17, 2025.

Relevance Rating: 4/5 — Highly relevant for the prevention layer of defensive strategy (reduces ability of ransomware actors to reach or download payloads). It’s not a detection/IR tool, so it complements but does not replace endpoint detection or backup strategies.

2) Citation: mitchellkrogza. (2025). nginx-ultimate-bad-bot-blocker. GitHub. https://github.com/mitchellkrogza/nginx-ultimate-bad-bot-blocker

Project Type: Security Tool / Nginx Blocking & Mitigation Framework

Synopsis:

This project supplies configuration files, lists, and installation scripts to block bad bots, malicious user-agents, spam referrers, vulnerability scanners, malware/adware domains, and other hostile web traffic at the Nginx level. It supports auto-install scripts, fail2ban integration, and manual configuration templates for rate limiting and IP/user-agent blocking. It’s valuable for ransomware defense because it helps harden public-facing web services, reducing attack surface and opportunistic scanning that can lead to exploitation.

Limitations: requires Nginx admin access to deploy, careful tuning to avoid blocking legitimate traffic, and ongoing updates to keep blocklists current. Project stats: ~4.5k stars, ~507 forks, active maintenance with many commits (version V4.2025.10.x).

Relevance Rating: 4/5 — Very relevant to perimeter hardening and reducing exposure to automated scanners and malicious crawlers that can discover vulnerabilities. Practical for organizations running Nginx-based services.