Cognitive Artifact Intelligence Research Network (CAIRN)

PRIMARY

Publisher	GitHub
Published	2026-09-22
Retrieved	2026-09-25
Cite key	github2026cognitive
URL	https://github.com/Cisco-Talos/Cognitive-Artifact-Intelligence-Research-Network

Repository confirmed live. Description: a research toolkit for identifying, attributing and tracking AI-related artefacts embedded in malware, using VirusTotal metadata exclusively.

Licence. MIT (Copyright (c) 2026 Cisco Systems, Inc.). **Language.** Python 3.11+.

Tiered YARA ontology - 26 rules across three tiers.

- T1, Primitive Artifacts (9 rules): individual cognitive signals such as API endpoints and hardcoded keys; "high recall, FPs expected".
- T2, Behavioral Context (8 rules): two or more co-occurring primitives in operationally meaningful combinations.
- T3, Operational Families (9 rules): family-level attribution anchored to confirmed seed hashes.

What it does not do. It "does not run YARA rules on raw binary content", and operates without binary downloads, file uploads to VirusTotal, URL submissions or active scans, scheduled automatic pulls, or touching malware directly.