

Instant Yara Signatures

RootCon 20
September 2026

How it started: Using AI to rewrite Yara-C

After RSAC in May 2026 I attempted to rewrite yara-c in golang. I was successful in learning how to leverage AI for programming. I wasn't successful in making yara-g faster. This is the story of that pivot.

1. Why rewrite open source projects?
2. Why it didn't work
3. Living through sophistry
4. Fail up
5. What I discovered: extremely fast way to write and detect a new kind of yara signature

Yara / IOCs and Detection

Yara / IOCs and Threat Intelligence

- Reverse Engineering and developing IOCs
- Types of Signatures: Cryptographic -vs- Detection
- Regex / Aho–Corasick and Ohh One Notation
- Yara-X rule execution optimization

Instant Signatures

- The goal: Ohh One $O(1)$
- Hilbert, Lanczos & Rotate
- 16 byte sketch

Reverse Engineering

recover a higher-level understanding of a program's components, structure, and behavior so that it can be understood, maintained, improved, interoperated with, or (in some cases) reproduced.

Humans Tools

Ida Pro, Ghidra, Binary Ninja, debuggers, triage tools

AI Tools

LLMs, Glasswing

Hashes -vs- Detections -vs- Entropy

Cryptographic hashes (sha1, sha265)

Detectors (EDR, Yara-*)

Multi Detectors (VirusTotal, [Abuse.ch](https://www.abuse.ch), OPSwat)

Sandboxes & AI RE

Fuzzy Hashes: PEHash, SimHash, ImpHash,

Yara

Developed by VT/Google

Has archived version in c99 (almost everyone use this)

New version in rust (almost zero commercial use)

Aho–Corasick and Regex

- Adding one signature slows scanning
- Most organizations scan my file type, grouping related signatures

Instant Yara Signatures (opensource)

Holloman3 (Hilbert + Lanczos + rotate)

Speed: 2.5 Gb/s

Written in assembly for X66 with AVX2 or arm NEON

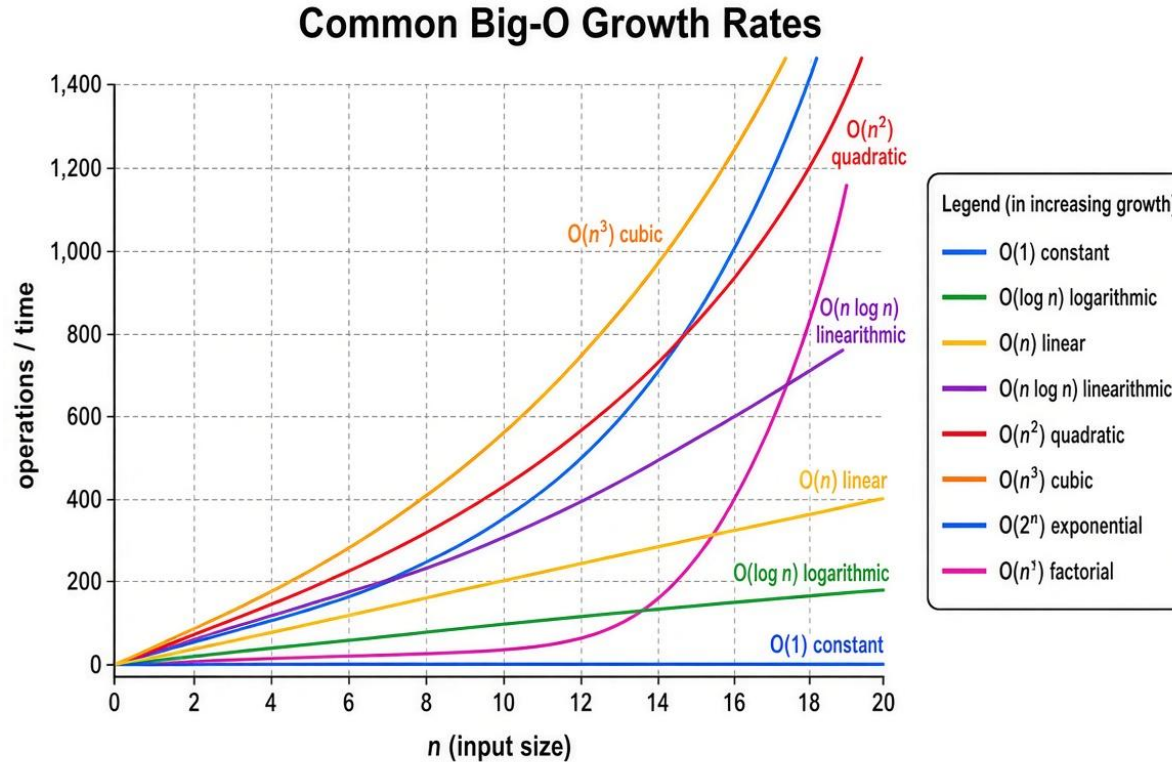
- Uses vector extensions

- 14 bit floating point (bfloat16)

- Designed for consumer hardware but also scales to GPUs and FPGAs

- Fast Identifier for any kind of object

Ohh One



Holloman3 Constant Time Sketches

Holloman3 is only three operations

- Mapping to a 2D Hilbert Curve
- Lanczos Resampling
- 90 Degree Rotation
- Results in a 128 bit vector represented as 32 hex chars

Things we accomplished since we answered this CFP

17 Opensource projects extending security tools to support instant signatures

Instant Siggen tool (assembly, c99, python, go, rust)

Email: Milter for Postfix and a Spamassassin module

Malware: Yara-c and Yara-x (crate) modules

Blockchain: Publish and Subscribe to data feeds of

- IPv4 , domain and URL feeds
- Holloman3 fingerprints for content of Phishing pages
- Holloman3 fingerprints for vt low-positives

Tool integration (cont)

Security Tools extended to support Instant Signatures

- Yara (c99) and Yara-x
- ClamAV
- Zeek (file based working on lookups from the block chain)

Working on modules/integrations

- Filigran (CTI tool)
- Arkime
- Suricutta

Any tool that uses yara [may] be able to use the above yara tools

Online malware scanning engine

Open source scanner that uses holloman3

Omega scan

- Calculates holloman3 and looks up attributes for the fingerprint
- Grpc over tls, fast
- trage tool

All tools are open source. Observe, Orient, Decide Act

Why

If we are entering a global cyber war, it would be nice to have tools and Threat Intelligence for everyone.

Opensource started with compiler and code tools because those are the building blocks for an internet.

We are building the tools for open source threat intelligence

Threat Chain: a blockchain for autonomous EDR tools

Blockchain is just the distribution mechanics not a token for money

Tools integrate with the chain for intelligence

Identity is pinned through DNSSEC, if you can trust the DNS then you can trust the crypto public keys to validate who published an IOC

Reputation is important, but being first is importanter; blockchains can help with reputation about trusting IOCs. Being first is an artifact of publishing.

IOCs have TTLS, its built into the chain, IPv4 attestations expire as do domains and URLs.

Threat Detection and publishing IOCs

Yesterday it took man hours to develop a publishable IOC.

Threat Hunting will become autonomous

Today writing an IOCs is a tool that consumes zero tokens

Tomorrow is about distributing IOCs for agentic tools

Questions

Rick Wesson

CEO, Support Intelligence Inc.

rick@organic.biz

[links to repos] [QR code for github]