



Features Business Explore Marketplace Pricing

This repository Search

Sign in or Sign up

InQuest / **awesome-yara**

Watch

38

★ Star

210

🍴 Fork

36

<> Code

Issues 0

Pull requests 0

Projects 0

Insights

Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

Sign up

Dismiss

A curated list of awesome YARA rules, tools, and people.

yara-rules

yara-signatures

yara

malware-rules

malware-analysis

malware-research

malware-detection

yara-scanner

yara-manager

threat-hunting

awesome

awesome-yara

awesome-list

ioc

📦 123 commits

🌿 1 branch

📦 0 releases

👤 5 contributors

Branch: master ▾





New pull request

Find file

Clone or download ▾

 rshipp Add @jheise yarascanner

Latest commit a12527f 5 days ago

 .travis.yml	Add awesome_bot config	7 months ago
 CONTRIBUTING.md	Add contributing file	2 months ago
 LICENSE	Initial commit	7 months ago
 README.md	Add @jheise yarascanner	5 days ago

README.md

Awesome YARA awesome

A curated list of awesome YARA rules, tools, and resources. Inspired by [awesome-python](#) and [awesome-php](#).

YARA is an acronym for: YARA: Another Recursive Acronym, or Yet Another Ridiculous Acronym. Pick your choice.

-- [Victor M. Alvarez \(@plusvic\)](#)

[YARA](#), the "pattern matching swiss knife for malware researchers (and everyone else)" is developed by [@plusvic](#) and [@VirusTotal](#). View it on [GitHub](#).

Contents

- [Awesome YARA](#)
 - [Rules](#)
 - [Tools](#)
 - [Services](#)
 - [People](#)
 - [Related Awesome Lists](#)

- [Contributing](#)

Legend

- 👁️ - Actively maintained, a repository worth watching.
- 💎 - Novel, interesting, educational, or otherwise stand-out content.
- ✨ - Recently released, shiny new toys.
- 🏆 - The biggest collection award, awarded to a single repo.



Rules

- [AlienVault Labs Rules](#)
 - Collection of tools, signatures, and rules from the researchers at [AlienVault Labs](#). Search the repo for .yar and .yara extensions to find about two dozen rules ranging from APT detection to generic sandbox / VM detection. Last updated in January of 2016.
- [Apple OSX](#)
 - Apple has ~40 YARA signatures for detecting malware on OSX. The file, XProtect.yara, is available locally at /System/Library/CoreServices/XProtect.bundle/Contents/Resources/.
- [bamfdetect rules](#)
 - Custom rules from Brian Wallace used for bamfdetect, along with some rules from other sources.
- [BinaryAlert YARA Rules](#) 👁️ ✨
 - A couple dozen rules written and released by AirBnB as part of their BinaryAlert tool (see next section). Detection for hack tools, malware, and ransomware across Linux, Window, and OS X. This is a new and active project.

- [Burp YARA Rules](#)
 - Collection of YARA rules intended to be used with the Burp Proxy through the Yara-Scanner extension. These rules focus mostly on non-exe malware typically delivered over HTTP including HTML, Java, Flash, Office, PDF, etc. Last updated in June of 2016.
- [Brian Carter Rules](#) ✨
 - Collection of personal rules written by Brian Carter, mostly designed for VirusTotal hunting.
- [CAPE Rules](#) 🙄
 - Rules from various authors bundled with the Config And Payload Extraction Cuckoo Sandbox extension (see next section).
- [CDI Rules](#) ✨
 - Collection of YARA rules released by [CyberDefenses](#) for public use. Built from information in intelligence profiles, dossiers and file work.
- [Citizen Lab Malware Signatures](#)
 - YARA signatures developed by Citizen Lab. Dozens of signatures covering a variety of malware families. The also include a syntax file for Vim. Last update was in November of 2016.
- [Didier Stevens Rules](#) 💎
 - Collection of rules from Didier Stevens, author of a suite of tools for inspecting OLE/RTF/PDF. Didier's rules are worth scrutinizing and are generally written purposed towards hunting. New rules are frequently announced through the [NVIISO Labs Blog](#).
- [ESET IOCs](#) 🙄

- Collection of YARA and Snort rules from IOCs collected by ESET researchers. There's about a dozen YARA Rules to glean from in this repo, search for file extension .yar. This repository is seemingly updated on a roughly monthly interval. New IOCs are often mentioned on the [ESET WeLiveSecurity Blog](#).
- [Fidelis Rules](#)
 - You can find a half dozen YARA rules in Fidelis Cyber's IOC repository. They update this repository on a roughly quarterly interval. Complete blog content is also available in this repository.
- [Florian Roth Rules](#) 👁️💎
 - Florian Roth's signature base is a frequently updated collection of IOCs and YARA rules that cover a wide range of threats. There are dozens of rules which are actively maintained. Watch the repository to see rules evolve over time to address false potives / negatives.
- [FSF Rules](#)
 - Mostly filetype detection rules, from the EmersonElectricCo FSF project (see next section).
- [GoDaddy ProcFilter Rules](#)
 - A couple dozen rules written and released by GoDaddy for use with ProcFilter (see next section). Example rules include detection for packers, mimikatz, and specific malware.
- [h3x2b Rules](#) 💎
 - Collection of signatures from h3x2b which stand out in that they are generic and can be used to assist in reverse engineering. There are YARA rules for identifying crypto routines, highly entropic sections (certificate discovery for example), discovering injection / hooking functionality, and more.
- [Icewater Rules](#)


- Repository of automatically generated YARA rules from Icewater.io. This repository is updated rapidly with newly generated signatures that mostly match on file size range and partial content hashes.
- [InQuest Rules](#) 👁️
- YARA rules published by InQuest researchers mostly geared towards threat hunting on Virus Total. Rules are updated as new samples are collected and novel pivots are discovered. The [InQuest Blog](#) will often discuss new findings.
- [kevthehermit Rules](#)
- Dozens of rules from the personal collection of Kevin Breen. This repository hasn't been updated since February of 2016.
- [NCC Group Rules](#) 👁️
- A handful of YARA rules released by NCC Group's Cyber Defence team.
- [Malice.IO YARA Plugin Rules](#) 👁️
- Collection of topical from a variety of sources for the YARA component of the Malice.IO framework.
- [mikesxrs YARA Rules Collection](#) 👁️ 🏆
- Large collection of open source rules aggregated from a variety of sources, including blogs and other more ephemeral sources. Over 100 categories, 1500 files, 4000 rules, and 20Mb. If you're going to pull down a single repo to play with, this is the one.
- [MrThreat Rules](#)
- Pubic repository of yara rules mainly used for osint and threat/counter intelligence.

- [Patrick Olsen Rules](#) 
 - Small collection of rules with a wide footprint for variety in detection. RATs, documents, PCAPs, executables, in-memory, point-of-sale malware, and more. Unfortunately this repository hasn't seen an update since late 2014.
- [QuickSand Lite Rules](#)
 - This repo contains a C framework and standalone tool for malware analysis, along with several useful YARA rules developed for use with the project.
- [SpiderLabs Rules](#)
 - Repository of tools and scripts related to malware analysis from the researchers at SpiderLabs. There's only three YARA rules here and the last update was back in 2015, but worth exploring.
- [Tenable Rules](#)
 - Small collection from Tenable Network Security.
- [TjadaNel Rules](#)
 - Small collection of malware rules.
- [VectraThreatLab Rules](#)
 - YARA rules for identifying anti-RE malware techniques.
- [x64dbg Signatures](#) 
 - Collection of interesting packer, compiler, and crypto identification signatures.
- [YARA-FORENSICS](#)

- Collection of file type identifying rules.
- [yara4pentesters](#)
 - Rules to identify files containing juicy information like usernames, passwords etc.
- [YaraRules Project Official Repo](#) 🙄
 - Large collection of rules constantly updated by the community.

Tools

- [AirBnB BinaryAlert](#)
 - Open-source serverless AWS pipeline where any file uploaded to an S3 bucket is immediately scanned with a configurable set of YARA rules.
- [bamfdetect](#)
 - Identifies and extracts information from bots and other malware.
- [CAPE: Config And Payload Extraction](#) 🙄
 - Extension of Cuckoo specifically designed to extract payloads and configuration from malware. CAPE can detect a number of malware techniques or behaviours, as well as specific malware families, from its initial run on a sample. This detection then triggers a second run with a specific package, in order to extract the malware payload and possibly its configuration, for further analysis.
- [CrowdStrike Feed Management System](#)
 - Framework for automating collection and processing of samples from VirusTotal, and executing commands based on YARA rule matches.
- [CSE-CST AssemblyLine](#) ✨
 - The Canadian Communications Security Establishment (CSE) open sourced [AssemblyLine](#), a platform for analyzing malicious files. The component linked here provides an interface to YARA.

- [ELAT](#)
 - Event Log Analysis Tool that creates/uses YARA rules for Windows event log analysis.
- [Emerson File Scanning Framework \(FSF\)](#)
 - Modular, recursive file scanning solution.
- [findcrypt-yara](#) and [FindYara](#)
 - IDA pro plugins to scan your binary with YARA rules to find crypto constants (and more).
- [GoDaddy ProcFilter](#) 
 - ProcFilter is a process filtering system for Windows with built-in YARA integration. YARA rules can be instrumented with custom meta tags that tailor its response to rule matches. It runs as a Windows service and is integrated with Microsoft's ETW API, making results viewable in the Windows Event Log. Installation, activation, and removal can be done dynamically and does not require a reboot.
- [go-yara](#)
 - Go bindings for YARA.
- [IDA_scripts](#)
 - IDA Python scripts for generating YARA sigs from executable opcodes (.NET included).
- [InQuest ThreatKB](#)
 - Knowledge base workflow management for YARA rules and C2 artifacts (IP, DNS, SSL).
- [iocextract](#)
 - Advanced Indicator of Compromise (IOC) extractor, with YARA rule extraction.
- [Invoke-Yara](#)
 - Powershell scripts to run YARA on remote machines.
- [KLara](#)
 - Distributed system written in Python, allows researchers to scan one or more YARA rules over collections with samples.
- [Laika BOSS](#)

- Object scanner and intrusion detection system that strives to achieve the following goals: Scalable, Flexible, Verbose.
 - [Whitepaper](#)
- [Loki](#)
 - Simple IOC and YARA rule scanner.
- [Malice](#)
 - Open source VirusTotal alternative, with YARA support.
- [MISP Threat Sharing](#)
 - Threat intelligence platform including indicators, threat intelligence, malware samples and binaries. Includes support for sharing, generating, and validating YARA signatures.
- [MITRE MultiScanner](#)
 - File analysis framework that assists the user in evaluating a set of files by automatically running a suite of tools for the user and aggregating the output.
- [node-yara](#)
 - YARA support for Node.js.
- [OCYara](#)
 - Performs OCR on image files and scans them for matches to YARA rules.
- [PasteHunter](#)
 - Scan pastebin.com with YARA rules.
- [Polichombr](#)
 - Collaborative malware analysis framework with YARA rule matching and other features.
- [VirusTotalTools](#)
 - Tools for checking samples against Virus Total, including VT_RuleMGR, for managing threat hunting YARA rules.
- [QuickSand.io](#)
 - Compact C framework to analyze suspected malware documents. Also includes a web interface and online analysis.
- [stoQ](#)

- Modular and highly customizable framework for the creation of data sets from multiple disparate data sources.
- [SwishDbgExt](#)
 - Microsoft WinDbg extension which includes the ability to use YARA rules to hunt processes in memory.
- [yabin](#)
 - Creates YARA signatures from executable code within malware.
- [yara-endpoint](#)
 - Tool useful for incident response as well as anti-malware endpoint based on YARA signatures.
- [YaraGenerator](#)
 - Quick, simple, and effective yara rule creation to isolate malware families and other malicious objects of interest.
- [YaraGen](#) and [yara_fn](#)
 - Plugins for x64dbg and IDAPython, respectively, that generate YARA rules from function blocks.
- [YaraGuardian](#)
 - Django web interface for managing YARA rules.
- [yaraMail](#)
 - YARA scanner for IMAP feeds and saved streams.
- [Yara Malware Quick menu scanner](#)
 - Adds the awesome YARA pattern scanner to Windows right click menus.
- [YaraManager](#)
 - Web based manager for YARA rules.
- [yarAnalyzer](#)
 - YARA rule set coverage analyzer.
- [yara-parser](#)
 - Tools for parsing rulesets using the exact grammar as YARA. Written in Go.
- [yaraPCAP](#)
 - YARA scanner For IMAP feeds and saved streams.
- [yara-procdump-python](#)

- Python extension to wrap the YARA process memory access API.
- [Yara Python ICAP Server](#)
 - ICAP server with YARA scanner.
- [Yara-Scanner](#)
 - Python-based extension that integrates a YARA scanner into Burp Suite.
- [yarascanner](#)
 - Golang-based web service to scan files with YARA rules.
- [Yara-Validator](#)
 - Validates YARA rules and tries to repair the broken ones.
- [yaraVT](#)
 - Scan files with Yara and send rule matches to VirusTotal reports as comments.
- [yarGen](#)
 - YARA rule generator for finding related samples and hunting.
- [Yeti](#)
 - Platform meant to organize observables, indicators of compromise, TTPs, and knowledge on threats in a single, unified repository.
- [yextend](#)
 - YARA integrated software to handle archive file data.

Services

- [MalShare](#)
 - Free malware repository providing researchers access to samples, malicious feeds, and YARA results.
- [MalwareConfig](#)
 - Extract IOCs from Remote Access Trojans.
- [YaraEditor \(Web\)](#)

- All-in-one website to create and manage YARA rules.
- [YaraRules Analyzer](#)
 - Upload and run files against rulesets from the YaraRules Project.
- [Yara Share](#)
 - Free repository and online community for users to upload and share Yara rules.

People

We're aggregating the Twitter handles for anyone involved with the projects on this page into a single list: [awesome-yara Twitter list](#). Do let us know if anyone is missing.

Related Awesome Lists

- [Crawler](#)
- [CVE PoC](#)
- [Forensics](#)
- [Hacking](#)
- [HackwithGithub](#)
- [Honeypots](#)
- [Incident-Response](#)
- [Infosec](#)
- [IOCs](#)
- [Malware Analysis](#)
- [ML for Cyber Security](#)
- [OSINT](#)

- [PCAP Tools](#)
- [Pentesting](#)
- [Reversing](#)
- [Security](#)
- [Static Analysis](#)
- [Threat Detection](#)
- [Threat Intelligence](#)

Contributing

See [CONTRIBUTING.md](#).

