

[Features](#)[Business](#)[Explore](#)[Marketplace](#)[Pricing](#)[This repository](#)[Sign in](#) or [Sign up](#) [sroberts](#) / [awesome-iocs](#) Watch

37

 Star

293

 Fork

52

 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 collection of sources of indicators of compromise

 19 commits 1 branch 0 releases 4 contributors MITBranch: **master** ▾[New pull request](#)[Find file](#)[Clone or download ▾](#)**sroberts** Merge pull request [#5](#) from rshipp/master ...

Latest commit 48b9c6b 18 days ago

 script	added basics for markdown ci	2 years ago
 .gitignore	don't need gitignore	2 years ago

 .mdlrc	added basics for markdown ci	2 years ago
 CONTRIBUTING.md	getting started	2 years ago
 Gemfile	added basics for markdown ci	2 years ago
 LICENSE.md	getting started	2 years ago
 README.md	Add iocextract to Tools section	19 days ago
 circle.yml	remove any ruby version reference to get the default	2 years ago

README.md

Awesome IOCs



An [awesome](#) collection of indicators of compromise (and a few IOC related tools).

IOCs

Indicators

- [0x27/linux.mirai](#)
- [botherder/targetedthreats](#)
- [circl/osint-feed](#)
- [citizenlab/malware-indicators](#)

- [da667/667s_Shitlist](#)
- [eset/malware-ioc](#)
- [fireeye/iocs](#)
- [jasonmiacono/IOCs](#)
- [makflwana/IOCs-in-CSV-format](#)
- [Neo23x0/signature-base](#)
- [pan-unit42/iocs](#)

Snort Signatures

- [Snort Downloads](#)
- [kingtuna/Signatures](#)

Yara Signatures

- [0pc0deFR/YaraRules](#)
- [citizenlab/malware-signatures](#)
- [kevthehermit/YaraRules](#)
- [OALabs/iocs](#)
- [sysforensics/YaraRules](#)
- [x64dbg/yarasigs](#)
- [Yara-Rules/rules](#)

Tools

IOC Tools

- [yahoo/PyIOCe](#)
- [mandiant/ioc_writer](#)
- [Neo23x0/yarGen](#)
- [InQuest/iocextract](#)

IOC Formats

- [mandiant/OpenIOC_1.1](#)
- [MISP Malware Information Sharing Platform & Threat Sharing format](#)
- [Mitre Cyber Observable eXpression \(CybOX™\)](#)
- [Mitre Malware Attribute Enumeration and Characterization \(MAEC™\)](#)
- [Mitre Structured Threat Information eXpression \(STIX™\)](#)
- [Yara](#)

