

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

345

 Star

1,858

 Fork

454

 Code Issues **2** Pull requests **2** 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 Threat Intelligence resources







[security](#)[awesome](#) **398** commits **52** branches **0** releases **38** contributors Apache-2.0Branch: **master** ▾[New pull request](#)[Find file](#)[Clone or download ▾](#)**hslatman** Merge pull request [#122](#) from villadso/master ...

Latest commit d07ce28 22 days ago

 [docs](#)

Provide mirror for deleted file

2 years ago

 <a href="#">.gitignore</a>	Add a gitignore; now .idea blacklisted only	2 years ago
 <a href="#">.travis.yml</a>	Update .travis.yml to allow SSL error and redirecting	6 months ago
 <a href="#">CONTRIBUTING.md</a>	Added contribution guidelines	2 years ago
 <a href="#">LICENSE</a>	Initial commit	2 years ago
 <a href="#">README.md</a>	Merge pull request #122 from villadso/master	22 days ago
 <a href="#">README_ch.md</a>	Chinese Translation update	25 days ago

## README.md

# awesome-threat-intelligence

---

A curated list of awesome Threat Intelligence resources

A concise definition of Threat Intelligence: *evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.*

Feel free to [contribute](#).

- [Sources](#)
- [Formats](#)
- [Frameworks & Platforms](#)
- [Tools](#)
- [Research, Standards & Books](#)

## Sources

Most of the resources listed below provide lists and/or APIs to obtain (hopefully) up-to-date information with regards to threats. Some consider these sources as threat intelligence, opinions differ however. A certain amount of (domain- or business-specific) analysis is necessary to create true threat intelligence.

<a href="#">Alexa Top 1 Million sites</a>	Probable Whitelist of the top 1 Million sites from Amazon(Alexa).
<a href="#">Apility.io</a>	Apility.io is a Minimal and Simple anti-abuse API blacklist lookup tool. It helps users to know immediately if an IP, Domain or Email is blacklisted. It automatically extracts all the information in realtime from multiple sources.
<a href="#">APT Groups and Operations</a>	A spreadsheet containing information and intelligence about APT groups, operations and tactics.
<a href="#">AutoShun</a>	A public service offering at most 2000 malicious IPs and some more resources.
<a href="#">BGP Ranking</a>	Ranking of ASNs having the most malicious content.
<a href="#">Botnet Tracker</a>	Tracks several active botnets.
<a href="#">BOTVRIJ.EU</a>	Botvrij.eu provides different sets of open source IOCs that you can use in your security devices to detect possible malicious activity.
<a href="#">BruteForceBlocker</a>	BruteForceBlocker is a perl script that monitors a server's sshd logs and identifies brute force attacks, which it then uses to automatically configure firewall blocking rules and submit those IPs back to the project site, <a href="http://danger.rulez.sk/projects/bruteforceblocker/blist.php">http://danger.rulez.sk/projects/bruteforceblocker/blist.php</a> .
<a href="#">C&amp;C Tracker</a>	A feed of known, active and non-sinkholed C&C IP addresses, from Bambenek Consulting.
<a href="#">CertStream</a>	Real-time certificate transparency log update stream. See SSL certificates as they're issued in

	real time.
<a href="#">CCSS Forum Malware Certificates</a>	The following is a list of digital certificates that have been reported by the forum as possibly being associated with malware to various certificate authorities. This information is intended to help prevent companies from using digital certificates to add legitimacy to malware and encourage prompt revocation of such certificates.
<a href="#">CI Army List</a>	A subset of the commercial <a href="#">CINS Score</a> list, focused on poorly rated IPs that are not currently present on other threatlists.
<a href="#">Cisco Umbrella</a>	Probable Whitelist of the top 1 million sites resolved by Cisco Umbrella (was OpenDNS).
<a href="#">Critical Stack Intel</a>	The free threat intelligence parsed and aggregated by Critical Stack is ready for use in any Bro production system. You can specify which feeds you trust and want to ingest.
<a href="#">C1fApp</a>	C1fApp is a threat feed aggregation application, providing a single feed, both Open Source and private. Provides statistics dashboard, open API for search and is been running for a few years now. Searches are on historical data.
<a href="#">Cymon</a>	Cymon is an aggregator of indicators from multiple sources with history, so you have a single interface to multiple threat feeds. It also provides an API to search a database along with a pretty web interface.
<a href="#">Disposable Email Domains</a>	A collection of anonymous or disposable email domains commonly used to spam/abuse services.
<a href="#">DNSTrails</a>	Free intelligence source for current and historical DNS information, WHOIS information, finding other websites associated with certain IPs, subdomain knowledge and technologies. There is a <a href="#">IP and domain intelligence API available</a> as well.
<a href="#">Emerging Threats Firewall Rules</a>	A collection of rules for several types of firewalls, including iptables, PF and PIX.

Emerging Threats IDS Rules	A collection of Snort and Suricata <i>rules</i> files that can be used for alerting or blocking.
ExoneraTor	The ExoneraTor service maintains a database of IP addresses that have been part of the Tor network. It answers the question whether there was a Tor relay running on a given IP address on a given date.
Exploitalert	Listing of latest exploits released.
Zeus Tracker	The Feodo Tracker <a href="#">abuse.ch</a> tracks the Feodo trojan.
FireHOL IP Lists	400+ publicly available IP Feeds analysed to document their evolution, geo-map, age of IPs, retention policy, overlaps. The site focuses on cyber crime (attacks, abuse, malware).
FraudGuard	FraudGuard is a service designed to provide an easy way to validate usage by continuously collecting and analyzing real-time internet traffic.
Grey Noise	Grey Noise is a system that collects and analyzes data on Internet-wide scanners. It collects data on benign scanners such as Shodan.io, as well as malicious actors like SSH and telnet worms.
Hail a TAXII	Hail a TAXII.com is a repository of Open Source Cyber Threat Intelligence feeds in STIX format. They offer several feeds, including some that are listed here already in a different format, like the Emerging Threats rules and PhishTank feeds.
HoneyDB	HoneyDB provides real time data of honeypot activity. This data comes from honeypots deployed on the Internet using the <a href="#">HoneyPy</a> honeypot. In addition, HoneyDB provides API access to collected honeypot activity, which also includes aggregated data from various honeypot Twitter feeds.
Icewater	12,805 Free Yara rules created by <a href="http://icewater.io">http://icewater.io</a>

<a href="#">Infosec - CERT-PA</a>	Malware samples <a href="#">collection and analysis</a> , <a href="#">blocklist service</a> , <a href="#">vulnerabilities database</a> and more. Created and managed my <a href="#">CERT-PA</a>
<a href="#">I-Blocklist</a>	I-Blocklist maintains several types of lists containing IP addresses belonging to various categories. Some of these main categories include countries, ISPs and organizations. Other lists include web attacks, TOR, spyware and proxies. Many are free to use, and available in various formats.
<a href="#">Majestic Million</a>	Probable Whitelist of the top 1 million web sites, as ranked by Majestic. Sites are ordered by the number of referring subnets. More about the ranking can be found on their <a href="#">blog</a> .
<a href="#">Malc0de DNS Sinkhole</a>	The files in this link will be updated daily with domains that have been indentified distributing malware during the past 30 days. Collected by malc0de.
<a href="#">MalShare.com</a>	The MalShare Project is a public malware repository that provides researchers free access to samples.
<a href="#">Malware Domain List</a>	A searchable list of malicious domains that also performs reverse lookups and lists registrants, focused on phishing, trojans, and exploit kits.
<a href="#">MalwareDomains.com</a>	The DNS-BH project creates and maintains a listing of domains that are known to be used to propagate malware and spyware. These can be used for detection as well as prevention (sinkholing DNS requests).
<a href="#">Metadefender.com</a>	Metadefender Cloud Threat Intelligence Feeds contains top new malware hash signatures, including MD5, SHA1, and SHA256. These new malicious hashes have been spotted by Metadefender Cloud within the last 24 hours. The feeds are updated daily with newly detected and reported malware to provide actionable and timely threat intelligence.
<a href="#">Minotaur</a>	The Minotaur Project is an ongoing research project by the team at NovCon Solutions (novcon.net). It is being built as a hub for security professionals, researchers and enthusiasts

	to discover new threats and discuss mitigations. It is a combination of 3rd-party opensource software, local datasets, new analysis tools, and more.
<a href="#">Netlab OpenData Project</a>	The Netlab OpenData project was presented to the public first at ISC' 2016 on August 16, 2016. We currently provide multiple data feeds, including DGA, EK, MalCon, Mirai C2, Mirai-Scanner, Hajime-Scanner and DRDoS Reflector.
<a href="#">NoThink!</a>	SNMP, SSH, Telnet Blacklisted IPs from Matteo Cantoni's Honeypots
<a href="#">NormShield Services</a>	NormShield Services provide thousands of domain information (including whois information) that potential phishing attacks may come from. Breach and blacklist services also available. There is free sign up for public services for continuous monitoring.
<a href="#">OpenPhish Feeds</a>	OpenPhish receives URLs from multiple streams and analyzes them using its proprietary phishing detection algorithms. There are free and commercial offerings available.
<a href="#">PhishTank</a>	PhishTank delivers a list of suspected phishing URLs. Their data comes from human reports, but they also ingest external feeds where possible. It's a free service, but registering for an API key is sometimes necessary.
<a href="#">Ransomware Tracker</a>	The Ransomware Tracker by <a href="#">abuse.ch</a> tracks and monitors the status of domain names, IP addresses and URLs that are associated with Ransomware, such as Botnet C&C servers, distribution sites and payment sites.
<a href="#">Rutgers Blacklisted IPs</a>	IP List of SSH Brute force attackers is created from a merged of locally observed IPs and 2 hours old IPs registered at badip.com and blocklist.de
<a href="#">SANS ICS Suspicious Domains</a>	The Suspicious Domains Threat Lists by <a href="#">SANS ICS</a> tracks suspicious domains. It offers 3 lists categorized as either <a href="#">high</a> , <a href="#">medium</a> or <a href="#">low</a> sensitivity, where the high sensitivity list has fewer false positives, whereas the low sensitivity list with more false positives. There is also an

	<a href="#">approved whitelist</a> of domains. Finally, there is a suggested <a href="#">IP blocklist</a> from <a href="#">DSshield</a> .
<a href="#">signature-base</a>	A database of signatures used in other tools by Neo23x0.
<a href="#">The Spamhaus project</a>	The Spamhaus Project contains multiple threatlists associated with spam and malware activity.
<a href="#">SSL Blacklist</a>	SSL Blacklist (SSLBL) is a project maintained by abuse.ch. The goal is to provide a list of "bad" SSL certificates identified by abuse.ch to be associated with malware or botnet activities. SSLBL relies on SHA1 fingerprints of malicious SSL certificates and offers various blacklists
<a href="#">Statvoo Top 1 Million Sites</a>	Probable Whitelist of the top 1 million web sites, as ranked by Statvoo.
<a href="#">Strongarm, by Percipient Networks</a>	Strongarm is a DNS blackhole that takes action on indicators of compromise by blocking malware command and control. Strongarm aggregates free indicator feeds, integrates with commercial feeds, utilizes Percipient's IOC feeds, and operates DNS resolvers and APIs for you to use to protect your network and business. Strongarm is free for personal use.
<a href="#">Talos Aspis</a>	Project Aspis is a closed collaboration between Talos and hosting providers to identify and deter major threat actors. Talos shares its expertise, resources, and capabilities including network and system forensics, reverse engineering, and threat intelligence at no cost to the provider.
<a href="#">Technical Blogs and Reports, by ThreatConnect</a>	This source is being populated with the content from over 90 open source, security blogs. IOCs ( <a href="#">Indicators of Compromise</a> ) are parsed out of each blog and the content of the blog is formatted in markdown.
<a href="#">Threatglass</a>	An online tool for sharing, browsing and analyzing web-based malware. Threatglass allows users to graphically browse website infections by viewing screenshots of the stages of



	infection, as well as by analyzing network characteristics such as host relationships and packet captures.
<a href="#">ThreatMiner</a>	ThreatMiner has been created to free analysts from data collection and to provide them a portal on which they can carry out their tasks, from reading reports to pivoting and data enrichment. The emphasis of ThreatMiner isn't just about indicators of compromise (IoC) but also to provide analysts with contextual information related to the IoC they are looking at.
<a href="#">WSTNPHX Malware Email Addresses</a>	Email addresses used by malware collected by VVestron Phoronix (WSTNPHX)
<a href="#">URLhaus</a>	URLhaus is a project from abuse.ch with the goal of sharing malicious URLs that are being used for malware distribution.
<a href="#">VirusShare</a>	VirusShare.com is a repository of malware samples to provide security researchers, incident responders, forensic analysts, and the morbidly curious access to samples of malicious code. Access to the site is granted via invitation only.
<a href="#">Yara-Rules</a>	An open source repository with different Yara signatures that are compiled, classified and kept as up to date as possible.
<a href="#">ZeuS Tracker</a>	The ZeuS Tracker by <a href="#">abuse.ch</a> tracks ZeuS Command & Control servers (hosts) around the world and provides you a domain- and a IP-blocklist.

## Formats

Standardized formats for sharing Threat Intelligence (mostly IOCs).

<a href="#">CAPEC</a>	The Common Attack Pattern Enumeration and Classification (CAPEC) is a comprehensive dictionary and classification taxonomy of known attacks that can be used by analysts, developers, testers, and educators
-----------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	to advance community understanding and enhance defenses.
CybOX	The Cyber Observable eXpression (CybOX) language provides a common structure for representing cyber observables across and among the operational areas of enterprise cyber security that improves the consistency, efficiency, and interoperability of deployed tools and processes, as well as increases overall situational awareness by enabling the potential for detailed automatable sharing, mapping, detection, and analysis heuristics.
IODEF (RFC5070)	The Incident Object Description Exchange Format (IODEF) defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents.
IDMEF (RFC4765)	<i>Experimental</i> - The purpose of the Intrusion Detection Message Exchange Format (IDMEF) is to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems and to the management systems that may need to interact with them.
MAEC	The Malware Attribute Enumeration and Characterization (MAEC) projects is aimed at creating and providing a standardized language for sharing structured information about malware based upon attributes such as behaviors, artifacts, and attack patterns.
OpenC2	OASIS Open Command and Control (OpenC2) Technical Committee. The OpenC2 TC will base its efforts on artifacts generated by the OpenC2 Forum. Prior to the creation of this TC and specification, the OpenC2 Forum was a community of cyber-security stakeholders that was facilitated by the National Security Agency (NSA). The OpenC2 TC was chartered to draft documents, specifications, lexicons or other artifacts to fulfill the needs of cyber security command and control in a standardized manner.
STIX 2.0	The Structured Threat Information eXpression (STIX) language is a standardized construct to represent cyber threat information. The STIX Language intends to convey the full range of potential cyber threat information and strives to be fully expressive, flexible, extensible, and automatable. STIX does not only allow tool-agnostic fields, but also provides so-called <i>test mechanisms</i> that provide means for embedding tool-specific elements, including OpenIOC, Yara and Snort. STIX 1.x has been archived <a href="#">here</a> .

TAXII	The Trusted Automated eXchange of Indicator Information (TAXII) standard defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries. TAXII defines concepts, protocols, and message exchanges to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats.
VERIS	The Vocabulary for Event Recording and Incident Sharing (VERIS) is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner. VERIS is a response to one of the most critical and persistent challenges in the security industry - a lack of quality information. In addition to providing a structured format, VERIS also collects data from the community to report on breaches in the Verizon Data Breach Investigations Report ( <a href="#">DBIR</a> ) and publishes this database online at <a href="#">VCDB.org</a> .

## Frameworks and Platforms

Frameworks, platforms and services for collecting, analyzing, creating and sharing Threat Intelligence.

AbuseHelper	AbuseHelper is an open-source framework for receiving and redistributing abuse feeds and threat intel.
AbuseIO	A toolkit to receive, process, correlate and notify end users about abuse reports, thereby consuming threat intelligence feeds.
AIS	The Department of Homeland Security's (DHS) free Automated Indicator Sharing (AIS) capability enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed. Threat indicators are pieces of information like malicious IP addresses or the sender address of a phishing email (although they can also be much more complicated).
Barncat	Fidelis Cybersecurity offers free access to Barncat after registration. The platform is intended to be

	used by CERTs, researchers, governments, ISPs and other, large organizations. The database holds various configuration settings used by attackers.
Bearded Avenger	The fastest way to consume threat intelligence. Successor to CIF.
Blueliv Threat Exchange Network	Allows participants to share threat indicators with the community.
CRITS	CRITS is a platform that provides analysts with the means to conduct collaborative research into malware and threats. It plugs into a centralized intelligence data repository, but can also be used as a private instance.
CIF	The Collective Intelligence Framework (CIF) allows you to combine known malicious threat information from many sources and use that information for IR, detection and mitigation. Code available on <a href="#">GitHub</a> .
IntelMQ	IntelMQ is a solution for CERTs for collecting and processing security feeds, pastebins, tweets using a message queue protocol. It's a community driven initiative called IHAP (Incident Handling Automation Project) which was conceptually designed by European CERTs during several InfoSec events. Its main goal is to give to incident responders an easy way to collect & process threat intelligence thus improving the incident handling processes of CERTs.
Interflow	Interflow is a security and threat information exchange platform created by Microsoft for professionals working in cybersecurity. It uses a distributed architecture which enables sharing of security and threat information within and between communities for a collectively stronger ecosystem. Offering multiple configuration options, Interflow allows users to decide what communities to form, what data feeds to consume, and with whom. Interflow is currently in private preview.

Malstrom	Malstrom aims to be a repository for threat tracking and forensic artifacts, but also stores YARA rules and notes for investigation.
ManaTI	The ManaTI project assists threat analyst by employing machine learning techniques that find new relationships and inferences automatically.
MANTIS	The Model-based Analysis of Threat Intelligence Sources (MANTIS) Cyber Threat Intelligence Management Framework supports the management of cyber threat intelligence expressed in various standard languages, like STIX and CybOX. It is <i>*not*</i> ready for large-scale production though.
Megatron	Megatron is a tool implemented by CERT-SE which collects and analyses bad IPs, can be used to calculate statistics, convert and analyze log files and in abuse & incident handling.
MineMeld	An extensible Threat Intelligence processing framework created Palo Alto Networks. It can be used to manipulate lists of indicators and transform and/or aggregate them for consumption by third party enforcement infrastructure.
MISP	The Malware Information Sharing Platform (MISP) is an open source software solution for collecting, storing, distributing and sharing cyber security indicators and malware analysis.
OpenIOC	OpenIOC is an open framework for sharing threat intelligence. It is designed to exchange threat information both internally and externally in a machine-digestible format.
OpenTAXII	OpenTAXII is a robust Python implementation of TAXII Services that delivers a rich feature set and a friendly Pythonic API built on top of a well designed application.
OSTrIcA	An open source plugin-oriented framework to collect and visualize Threat Intelligence information.
OTX - Open Threat Exchange	AlienVault Open Threat Exchange (OTX) provides open access to a global community of threat researchers and security professionals. It delivers community-generated threat data, enables collaborative research, and automates the process of updating your security infrastructure with threat data from any source.

<a href="#">Open Threat Partner eXchange</a>	The Open Threat Partner eXchange (OpenTPX) consists of an open-source format and tools for exchanging machine-readable threat intelligence and network security operations data. It is a JSON-based format that allows sharing of data between connected systems.
<a href="#">PassiveTotal</a>	The PassiveTotal platform offered by RiskIQ is a threat-analysis platform which provides analysts with as much data as possible in order to prevent attacks before they happen. Several types of solutions are offered, as well as integrations (APIs) with other systems.
<a href="#">Pulsedive</a>	Pulsedive is a free, community threat intelligence platform that is consuming open-source feeds, enriching the IOCs, and running them through a risk-scoring algorithm to improve the quality of the data. It allows users to submit, search, correlate, and update IOCs; lists "risk factors" for why IOCs are higher risk; and provides a high level view of threats and threat activity.
<a href="#">Recorded Future</a>	Recorded Future is a premium SaaS product that automatically unifies threat intelligence from open, closed, and technical sources into a single solution. Their technology uses natural language processing (NLP) and machine learning to deliver that threat intelligence in real time — making Recorded Future a popular choice for IT security teams.
<a href="#">Scumblr</a>	Scumblr is a web application that allows performing periodic syncs of data sources (such as Github repositories and URLs) and performing analysis (such as static analysis, dynamic checks, and metadata collection) on the identified results. Scumblr helps you streamline proactive security through an intelligent automation framework to help you identify, track, and resolve security issues faster.
<a href="#">Soltra Edge</a>	The basic version of Soltra Edge is available for free. It supports a community defense model that is highly interoperable and extensible. It is built with industry standards supported out of the box, including STIX and TAXII.
<a href="#">STAXX (Anomali)</a>	Anomali STAXX™ gives you a free, easy way to subscribe to any STIX/TAXII feed. Simply download the STAXX client, configure your data sources, and STAXX will handle the rest.

<a href="#">stoQ</a>	stoQ is a framework that allows cyber analysts to organize and automate repetitive, data-driven tasks. It features plugins for many other systems to interact with. One use case is the extraction of IOCs from documents, an example of which is shown <a href="#">here</a> , but it can also be used for deobfuscation and decoding of content and automated scanning with YARA, for example.
<a href="#">TARDIS</a>	The Threat Analysis, Reconnaissance, and Data Intelligence System (TARDIS) is an open source framework for performing historical searches using attack signatures.
<a href="#">ThreatConnect</a>	ThreatConnect is a platform with threat intelligence, analytics, and orchestration capabilities. It is designed to help you collect data, produce intelligence, share it with others, and take action on it.
<a href="#">ThreatCrowd</a>	ThreatCrowd is a system for finding and researching artefacts relating to cyber threats.
<a href="#">ThreatExchange</a>	Facebook created ThreatExchange so that participating organizations can share threat data using a convenient, structured, and easy-to-use API that provides privacy controls to enable sharing with only desired groups. This project is still in <b>beta</b> . Reference code can be found at <a href="#">GitHub</a> .
<a href="#">Threat_Note</a>	DPS' Lightweight Investigation Notebook.
<a href="#">XFE - X-Force Exchange</a>	The X-Force Exchange (XFE) by IBM XFE is a free SaaS product that you can use to search for threat intelligence information, collect your findings, and share your insights with other members of the XFE community.
<a href="#">Yara Share</a>	Yara Share is an online Yara rule editor and sharing platform.
<a href="#">Yeti</a>	The open, distributed, machine and analyst-friendly threat intelligence repository. Made by and for incident responders.

## Tools

All kinds of tools for parsing, creating and editing Threat Intelligence. Mostly IOC based.

<a href="#">ActorTrackr</a>	ActorTrackr is an open source web application for storing/searching/linking actor related data. The primary sources are from users and various public repositories. Source available on <a href="#">GitHub</a> .
<a href="#">AIEngine</a>	AIEngine is a next generation interactive/programmable Python/Ruby/Java/Lua packet inspection engine with capabilities of learning without any human intervention, NIDS(Network Intrusion Detection System) functionality, DNS domain classification, network collector, network forensics and many others. Source available on <a href="#">Bitbucket</a> .
<a href="#">Automater</a>	Automater is a URL/Domain, IP Address, and Md5 Hash OSINT tool aimed at making the analysis process easier for intrusion Analysts.
<a href="#">BotScout</a>	BotScout helps prevent automated web scripts, known as "bots", from registering on forums, polluting databases, spreading spam, and abusing forms on web sites.
<a href="#">bro-intel-generator</a>	Script for generating Bro intel files from pdf or html reports.
<a href="#">cabby</a>	A simple Python library for interacting with TAXII servers.
<a href="#">cacador</a>	Cacador is a tool written in Go for extracting common indicators of compromise from a block of text.
<a href="#">Combine</a>	Combine gathers Threat Intelligence Feeds from publicly available sources.
<a href="#">CrowdFMS</a>	CrowdFMS is a framework for automating collection and processing of samples from VirusTotal, by leveraging the Private API system. The framework automatically downloads recent samples, which triggered an alert on the users YARA notification feed.
<a href="#">CyBot</a>	CyBot is a threat intelligence chat bot. It can perform several types of lookups offered by custom modules.
<a href="#">Cuckoo Sandbox</a>	Cuckoo Sandbox is an automated dynamic malware analysis system. It's the most well-known



	open source malware analysis sandbox around and is frequently deployed by researchers, CERT/SOC teams, and threat intelligence teams all around the globe. For many organizations Cuckoo Sandbox provides a first insight into potential malware samples.
<a href="#">Fenrir</a>	Simple Bash IOC Scanner.
<a href="#">FireHOL IP Aggregator</a>	Application for keeping feeds from FireHOL <a href="#">blocklist-ipsets</a> (only *.netset and *.ipset files are aggregated) in PostgreSQL with including historical changes. For requests developed HTTP-based API service.
<a href="#">Forager</a>	Multithreaded threat intelligence hunter-gatherer script.
<a href="#">GoatRider</a>	GoatRider is a simple tool that will dynamically pull down Artillery Threat Intelligence Feeds, TOR, AlienVaults OTX, and the Alexa top 1 million websites and do a comparison to a hostname file or IP file.
<a href="#">Google APT Search Engine</a>	APT Groups, Operations and Malware Search Engine. The sources used for this Google Custom Search are listed on <a href="#">GitHub gist</a> .
<a href="#">GOSINT</a>	The GOSINT framework is a free project used for collecting, processing, and exporting high quality public indicators of compromise (IOCs).
<a href="#">hashdd</a>	A tool to lookup related information from cryptographic hash value
<a href="#">Harbinger Threat Intelligence</a>	Python script that allows to query multiple online threat aggregators from a single interface.
<a href="#">Hiryu</a>	A tool to organize APT campaign information and to visualize relations between IOCs.
<a href="#">IOC Editor</a>	A free editor for Indicators of Compromise (IOCs).
<a href="#">ioc_parser</a>	Tool to extract indicators of compromise from security reports in PDF format.

<a href="#">ioc_writer</a>	Provides a Python library that allows for basic creation and editing of OpenIOC objects.
<a href="#">IOCextractor</a>	IOC (Indicator of Compromise) Extractor is a program to help extract IOCs from text files. The general goal is to speed up the process of parsing structured data (IOCs) from unstructured or semi-structured data
<a href="#">ibmxforceex.checker.py</a>	Python client for the IBM X-Force Exchange.
<a href="#">jager</a>	Jager is a tool for pulling useful IOCs (indicators of compromise) out of various input sources (PDFs for now, plain text really soon, webpages eventually) and putting them into an easy to manipulate JSON format.
<a href="#">libtaxii</a>	A Python library for handling TAXII Messages invoking TAXII Services.
<a href="#">Loki</a>	Simple IOC and Incident Response Scanner.
<a href="#">LookUp</a>	LookUp is a centralized page to get various threat information about an IP address. It can be integrated easily into context menus of tools like SIEMs and other investigative tools.
<a href="#">Machinae</a>	Machinae is a tool for collecting intelligence from public sites/feeds about various security-related pieces of data: IP addresses, domain names, URLs, email addresses, file hashes and SSL fingerprints.
<a href="#">MISP Workbench</a>	Tools to export data out of the MISP MySQL database and use and abuse them outside of this platform.
<a href="#">MISP-Taxii-Server</a>	A set of configuration files to use with EclecticIQ's OpenTAXII implementation, along with a callback for when data is sent to the TAXII Server's inbox.
<a href="#">nyx</a>	The goal of this project is to facilitate distribution of Threat Intelligence artifacts to defensive systems and to enhance the value derived from both open source and commercial tools.
<a href="#">openioc-to-stix</a>	Generate STIX XML from OpenIOC XML.

<a href="#">OSTIP</a>	A homebrew threat data platform.
<a href="#">poortego</a>	Open-source project to handle the storage and linking of open-source intelligence (ala Maltego, but free as in beer and not tied to a specific / proprietary database). Originally developed in ruby, but new codebase completely rewritten in python.
<a href="#">PyIOCe</a>	PyIOCe is an IOC editor written in Python.
<a href="#">QRadio</a>	QRadio is a tool/framework designed to consolidate cyber threats intelligence sources. The goal of the project is to establish a robust modular framework for extraction of intelligence data from vetted sources.
<a href="#">rastrea2r</a>	Collecting & Hunting for Indicators of Compromise (IOC) with gusto and style!
<a href="#">Redline</a>	A host investigations tool that can be used for, amongst others, IOC analysis.
<a href="#">RITA</a>	Real Intelligence Threat Analytics (RITA) is intended to help in the search for indicators of compromise in enterprise networks of varying size.
<a href="#">stix-viz</a>	STIX Visualization Tool.
<a href="#">TAXII Test Server</a>	Allows you to test your TAXII environment by connecting to the provided services and performing the different functions as written in the TAXII specifications.
<a href="#">threataggregator</a>	ThreatAggregator aggregates security threats from a number of online sources, and outputs to various formats, including CEF, Snort and IPTables rules.
<a href="#">threatcrowd_api</a>	Python Library for ThreatCrowd's API.
<a href="#">threatcmd</a>	Cli interface to ThreatCrowd.
<a href="#">Threatelligence</a>	Threatelligence is a simple cyber threat intelligence feed collector, using Elasticsearch, Kibana and Python to automatically collect intelligence from custom or public sources.

	Automatically updates feeds and tries to further enhance data for dashboards. Projects seem to be no longer maintained, however.
<a href="#">ThreatPinch Lookup</a>	An extension for Chrome that creates hover popups on every page for IPv4, MD5, SHA2, and CVEs. It can be used for lookups during threat investigations.
<a href="#">ThreatScanner</a>	ThreatScanner by Fidelis Cybersecurity runs a script to hunt for IOCs or YARA rules on a single machine and automatically generates a report that provides details of suspicious artifacts.
<a href="#">ThreatTracker</a>	A Python script designed to monitor and generate alerts on given sets of IOCs indexed by a set of Google Custom Search Engines.
<a href="#">threat_intel</a>	Several APIs for Threat Intelligence integrated in a single package. Included are: OpenDNS Investigate, VirusTotal and ShadowServer.
<a href="#">Threat-Intelligence-Hunter</a>	TIH is an intelligence tool that helps you in searching for IOCs across multiple openly available security feeds and some well known APIs. The idea behind the tool is to facilitate searching and storing of frequently added IOCs for creating your own local database of indicators.
<a href="#">tiq-test</a>	The Threat Intelligence Quotient (TIQ) Test tool provides visualization and statistical analysis of TI feeds.
<a href="#">YETI</a>	YETI is a proof-of-concept implementation of TAXII that supports the Inbox, Poll and Discovery services defined by the TAXII Services Specification.
<a href="#">sqhunter</a>	Threat hunter based on osquery, Salt Open and Cymon API. It can query open network sockets and check them against threat intelligence sources

## Research, Standards & Books

All kinds of reading material about Threat Intelligence. Includes (scientific) research and whitepapers.

<a href="#">APT &amp; Cyber Criminal Campaign Collection</a>	Extensive collection of (historic) campaigns. Entries come from various sources.
<a href="#">APTnotes</a>	A great collection of sources regarding <i>Advanced Persistent Threats</i> (APTs). These reports usually include strategic and tactical knowledge or advice.
<a href="#">ATT&amp;CK</a>	Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a model and framework for describing the actions an adversary may take while operating within an enterprise network. ATT&CK is a constantly growing common reference for post-access techniques that brings greater awareness of what actions may be seen during a network intrusion. MITRE is actively working on integrating with related construct, such as CAPEC, STIX and MAEC.
<a href="#">Building Threat Hunting Strategies with the Diamond Model</a>	Blogpost by Sergio Caltagirone on how to develop intelligent threat hunting strategies by using the Diamond Model.
<a href="#">Cyber Analytics Repository by MITRE</a>	The Cyber Analytics Repository (CAR) is a knowledge base of analytics developed by MITRE based on the Adversary Tactics, Techniques, and Common Knowledge (ATT&CK™) threat model.
<a href="#">Definitive Guide to Cyber Threat Intelligence</a>	Describes the elements of cyber threat intelligence and discusses how it is collected, analyzed, and used by a variety of human and technology consumers. Further examines how intelligence can improve cybersecurity at tactical, operational, and strategic levels, and how it can help you stop attacks sooner, improve your defenses, and talk more productively about cybersecurity issues with executive management in typical <i>for Dummies</i> style.
<a href="#">The Detection</a>	The DML model is a capability maturity model for referencing ones maturity in detecting cyber

<a href="#">Maturity Level (DML)</a>	attacks. It's designed for organizations who perform intel-driven detection and response and who put an emphasis on having a mature detection program. The maturity of an organization is not measured by it's ability to merely obtain relevant intelligence, but rather it's capacity to apply that intelligence effectively to detection and response functions.
<a href="#">The Diamond Model of Intrusion Analysis</a>	This paper presents the Diamond Model, a cognitive framework and analytic instrument to support and improve intrusion analysis. Supporting increased measurability, testability and repeatability in intrusion analysis in order to attain higher effectivity, efficiency and accuracy in defeating adversaries is one of its main contributions.
<a href="#">F3EAD</a>	F3EAD is a military methodology for combining operations and intelligence.
<a href="#">Guide to Cyber Threat Information Sharing by NIST</a>	The Guide to Cyber Threat Information Sharing (NIST Special Publication 800-150) assists organizations in establishing computer security incident response capabilities that leverage the collective knowledge, experience, and abilities of their partners by actively sharing threat intelligence and ongoing coordination. The guide provides guidelines for coordinated incident handling, including producing and consuming data, participating in information sharing communities, and protecting incident-related data.
<a href="#">Intelligence Preparation of the Battlefield/Battlespace</a>	This publication discusses intelligence preparation of the battlespace (IPB) as a critical component of the military decision making and planning process and how IPB supports decision making, as well as integrating processes and continuing activities.
<a href="#">Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains</a>	The intrusion kill chain as presented in this paper provides one with a structured approach to intrusion analysis, indicator extraction and performing defensive actions.
<a href="#">ISAO Standards</a>	The ISAO Standards Organization is a non-governmental organization established on October

Organization	1, 2015. Its mission is to improve the Nation's cybersecurity posture by identifying standards and guidelines for robust and effective information sharing related to cybersecurity risks, incidents, and best practices.
Joint Publication 2-0: Joint Intelligence	This publication by the U.S army forms the core of joint intelligence doctrine and lays the foundation to fully integrate operations, plans and intelligence into a cohesive team. The concepts presented are applicable to (Cyber) Threat Intelligence too.
Microsoft Research Paper	A framework for cybersecurity information sharing and risk reduction. A high level overview paper by Microsoft.
MISP Core Format (draft)	This document describes the MISP core format used to exchange indicators and threat information between MISP (Malware Information and threat Sharing Platform) instances.
NECOMA Project	The Nippon-European Cyberdefense-Oriented Multilayer threat Analysis (NECOMA) research project is aimed at improving threat data collection and analysis to develop and demonstrate new cyberdefense mechanisms. As part of the project several publications and software projects have been published.
Pyramid of Pain	The Pyramid of Pain is a graphical way to express the difficulty of obtaining different levels of indicators and the amount of resources adversaries have to expend when obtained by defenders.
Structured Analytic Techniques For Intelligence Analysis	This book contains methods that represent the most current best practices in intelligence, law enforcement, homeland security, and business analysis.
Threat Intelligence: Collecting, Analysing, Evaluating	This report by MWR InfoSecurity clearly describes several different types of threat intelligence, including strategic, tactical and operational variations. It also discusses the processes of requirements elicitation, collection, analysis, production and evaluation of threat intelligence.

	Also included are some quick wins and a maturity model for each of the types of threat intelligence defined by MWR InfoSecurity.
<a href="#">Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives</a>	A systematic study of 22 Threat Intelligence Sharing Platforms (TISP) surfacing eight key findings about the current state of threat intelligence usage, its definition and TISPs.
<a href="#">Traffic Light Protocol</a>	The Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the correct audience. It employs four colors to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s).
<a href="#">Who's Using Cyberthreat Intelligence and How?</a>	A whitepaper by the SANS Institute describing the usage of Threat Intelligence including a survey that was performed.
<a href="#">WOMBAT Project</a>	The WOMBAT project aims at providing new means to understand the existing and emerging threats that are targeting the Internet economy and the net citizens. To reach this goal, the proposal includes three key workpackages: (i) real time gathering of a diverse set of security related raw data, (ii) enrichment of this input by means of various analysis techniques, and (iii) root cause identification and understanding of the phenomena under scrutiny.

## License

Licensed under [Apache License 2.0](#).



