📖 ninoseki / **mitaka**

◉ Watch 17   ★ Star 246   ⑂ Fork 29

<> Code   ⓘ Issues **5**   ⑂ Pull requests **1**   ▥ Projects **0**   🛡 Security   📊 Insights

Join GitHub today

Dismiss

GitHub is home to over 40 million developers working together to host and review code, manage projects, and build software together.

Sign up

A browser extension for OSINT search   https://ninoseki.github.io/projects/m…

chrome-extension   security   threat-intelligence   osint

🕐 **637** commits   ⑂ **1** branch   📦 **0** packages   🏷 **26** releases   👥 **2** contributors   ⚖ MIT

Branch: master ⌄   New pull request   Find file   Clone or download ⌄

🐸 **ninoseki** Merge pull request #339 from ninoseki/update-dependencies ⋯   Latest commit bb7393f 13 hours ago

📁 examples	docs: update README.md	11 months ago
📁 scripts	chore: update Webpack settings	5 months ago
📁 src	refactor: minor changes in UI	6 days ago
📁 test	feat: add URLhaus lookup	9 days ago
📄 .eslintrc	Revert "chore: add eslint-plugin-mocha"	24 days ago
📄 .gitignore	chore: update Webpack settings	5 months ago
📄 .prettierrc	refactor: auto format by prettier	9 months ago
📄 .travis.yml	chore: update travis.yml	4 months ago
📄 LICENSE	Initial commit	2 years ago
📄 README.md	chore: migrate to travis-ci.com	9 days ago
📄 package-lock.json	chore: update dependencies	13 hours ago
📄 package.json	chore: update dependencies	13 hours ago
📄 tsconfig.json	chore: move spec from src to root	3 months ago
📄 webpack.config.js	chore: update Webpack performance config	8 days ago

📖 **README.md**

Mitaka

build passing   codefactor A   coverage 95%

Extract   Refang   Search/Scan!

Mitaka is a browser extension for OSINT search which can:

- Extract & refang IoC from a selected block of text.
  - E.g. `example[.]com` to `example.com`, `test[at]example.com` to `test@example.com`, `hxxp://example.com` to `http://example.com`, etc.
- Search / scan it on various engines.
  - E.g. VirusTotal, urlscan.io, Censys, Shodan, etc.

Features

Supported IOC types

name	desc.	e.g.
text	Freetext	any string(s)
ip	IPv4 address	`8.8.8.8`
domain	Domain name	`github.com`
url	URL	`https://github.com`
email	Email address	`test@test.com`
asn	ASN	`AS13335`
hash	md5 / sha1 / sha256	`44d88612fea8a8f36de82e1278abb02f`
cve	CVE number	`CVE-2018-11776`
btc	BTC address	`1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa`
gaPubID	Google Adsense Publisher ID	`pub-9383614236930773`
gaTrackID	Google Analytics Tracker ID	`UA-67609351-1`

Supported search engines

name	url	supported types
AbuseIPDB	https://www.abuseipdb.com	ip
Apility	https://apility.io	ip / domain / email / asn
apklab	https://apklab.io	hash (SHA256 only)
archive.org	https://archive.org	url
archive.today	http://archive.fo	url
BGPView	https://bgpview.io	ip / asn
BinaryEdge	https://app.binaryedge.io	ip / domain
BitcoinAbuse	https://www.bitcoinabuse.com	btc
BitcoinWhosWhos	https://bitcoinwhoswho.com	btc
Blockchain.com	https://www.blockchain.com	btc
BlockCypher	https://live.blockcypher.com	btc
Censys	https://censys.io	ip / domain / asn / text
crt.sh	https://crt.sh	domain
DNSlytics	https://dnslytics.com	ip / domain
DomainBigData	https://domainbigdata.com	ip / domain / email
DomainTools	https://www.domaintools.com	ip / domain
DomainWatch	https://domainwat.ch	domain / email
EmailRep	https://emailrep.io	email

name	url	supported types
FindSubDomains	https://findsubdomains.com	domain
FOFA	https://fofa.so	ip / domain
FortiGuard	https://fortiguard.com	ip / url / cve
Google Safe Browsing	https://transparencyreport.google.com	domain / url
GreyNoise	https://viz.greynoise.io	ip / domain / asn
Hashdd	https://hashdd.com	ip / domain / hash
HybridAnalysis	https://www.hybrid-analysis.com	ip / domain / hash
Intelligence X	https://intelx.io	ip / domain / url / email / btc
IPinfo	https://ipinfo.io	ip / asn
IPIP	https://en.ipip.net	ip / asn
Joe Sandbox	https://www.joesandbox.com	hash
MalShare	https://malshare.com	hash
Maltiverse	https://www.maltiverse.com	domain / hash
NVD	https://nvd.nist.gov	cve
OOCPR	https://data.occrp.org	email
ONYPHE	https://www.onyphe.io	ip
OpenTIP	https://opentip.kaspersky.com	hash
OTX	https://otx.alienvault.com	ip / domain / hash
PubDB	http://pub-db.com	gaPubID / gaTrackID
PublicWWW	https://publicwww.com	text
Pulsedive	https://pulsedive.com	ip / domaion / url / hash
RiskIQ	http://community.riskiq.com	ip / domain / email / gaTrackID
Scumware	https://www.scumware.org	ip / domain / hash (MD5 only)
SecurityTrails	https://securitytrails.com	ip / domain / email
Shodan	https://www.shodan.io	ip / domain / asn
Sploitus	https://sploitus.com	cve
SpyOnWeb	http://spyonweb.com	ip / domain / gaPubID / gaTrackID
Talos	https://talosintelligence.com	ip / domain
ThreatConnect	https://app.threatconnect.com	ip / domain / email
ThreatCrowd	https://www.threatcrowd.org	ip / domain / email
ThreatMiner	https://www.threatminer.org	ip / domain / hash
TIP	https://threatintelligenceplatform.com	ip / domain
URLhaus	https://urlhaus.abuse.ch	ip / domain
Urlscan	https://urlscan.io	ip / domain / asn / url
ViewDNS	https://viewdns.info	ip / domain / email
VirusTotal	https://www.virustotal.com	ip / domain / url / hash
Vulmon	https://vulmon.com	cve
VulncodeDB	https://www.vulncode-db.com	cve

name	url	supported types
VxCube	http://vxcube.com	ip / domain / hash
WebAnalyzer	https://wa-com.com	domain
We Leak Info	https://weleakinfo.com	email
X-Force Exchange	https://exchange.xforce.ibmcloud.com	ip / domain / hash
ZoomEye	https://www.zoomeye.org	ip

Supported scan engines

name	url	supported types
Urlscan	https://urlscan.io	ip / domain / url
VirusTotal	https://www.virustotal.com	url

Downloads

Browser	Link	Users	Rating
Google Chrome	chrome web store v0.64.0	users 1.7k	rating 5/5
Firefox	mozilla add-on v0.65.0	users 201	rating 5/5

How to use

This browser extension shows context menus based on a type of IoC you selected and then you can choose what you want to search / scan on.
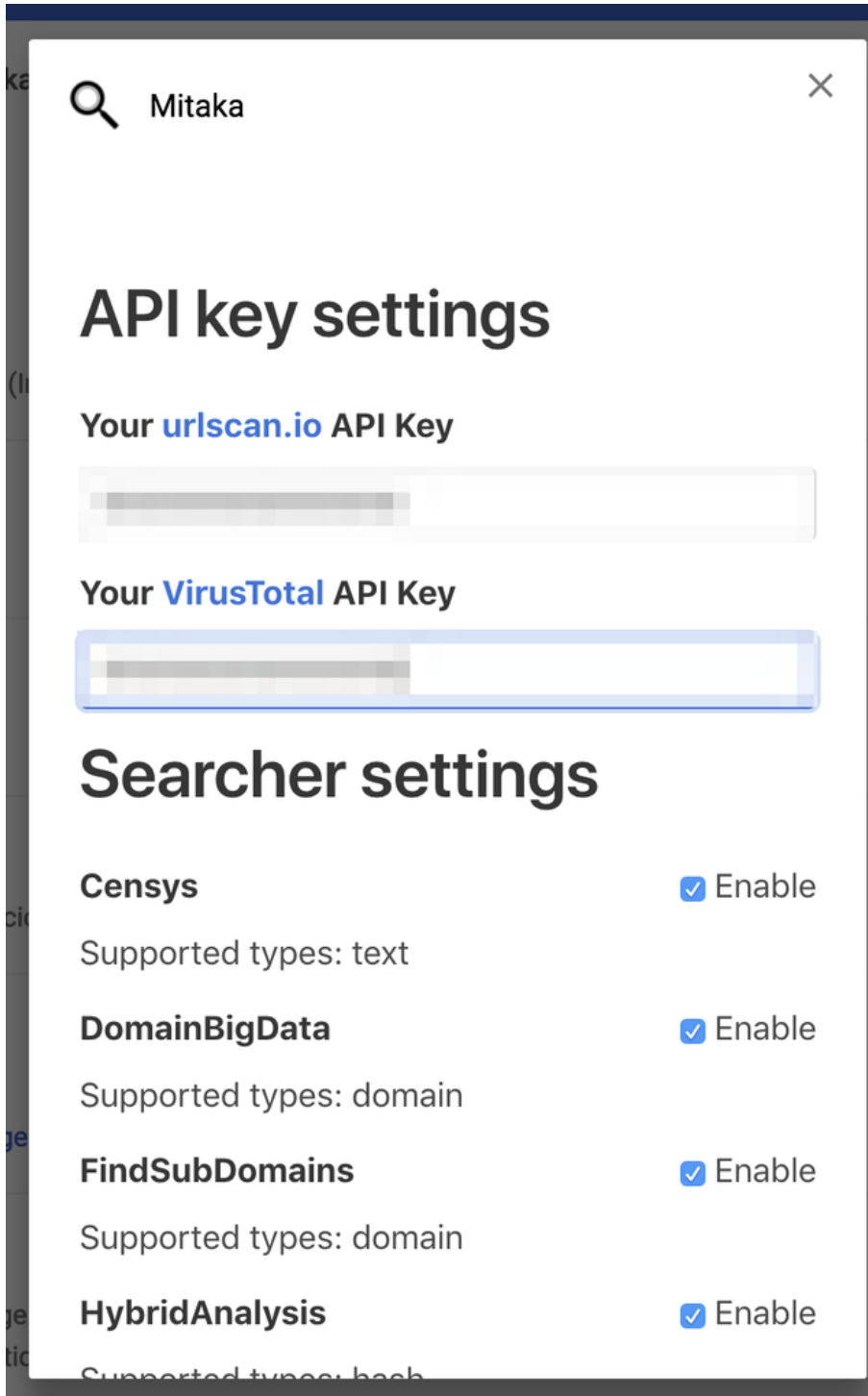
Examples:
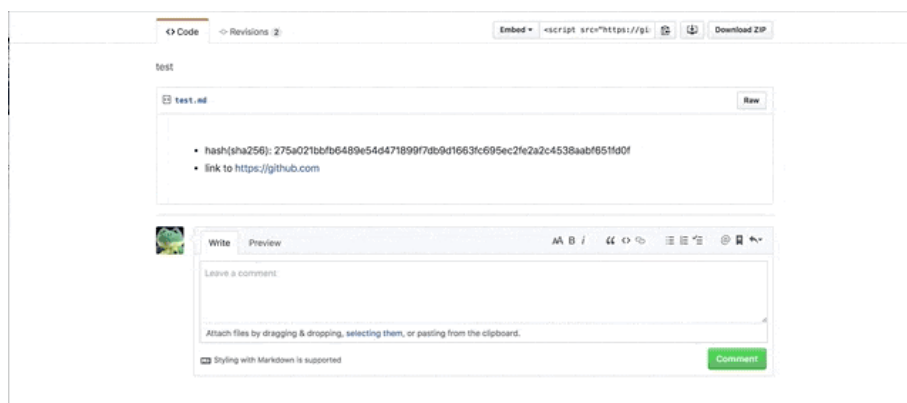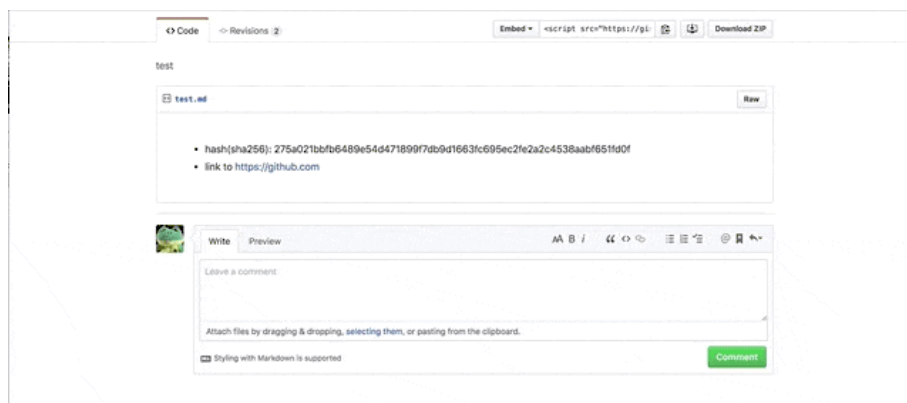
Note:

Please set your urlscan.io & VirusTotal API keys in the options page for enabling urlscan.io & VirusTotal scans.

Options

You can enable / disable a search engine on the options page based on your preference.

About Permissons

This browser extension requires the following permissions.

- `Read and change all your data on the websites you visit`:
  - This extension creates context menus dynamically based on what you select on a website.
  - It means this extension requires reading all your data on the websites you visit. (This extension doesn't change anything on the websites)
- `Display notifications`:
  - This extension makes a notification when something goes wrong.

I don't (and will never) collect any information from the users.

Alternatives or Similar Tools

- CrowdScrape
- Gotanda
- Sputnik
- ThreatConnect Integrated Chrome Extension
- ThreatPinch Lookup
- VTchromizer

How to build (for developers)

This browser extension is written in TypeScript and built by webpack.

TypeScript files will start out in `src` directory, run through the TypeScript compiler, then webpack, and end up in JavaScript files in `dist` directory.

```
git clone https://github.com/ninoseki/mitaka.git
cd mitaka
npm install
npm run test
npm run build
```

For loading an unpacked extension, please follow the procedures described at https://developer.chrome.com/extensions/getstarted.

Misc

Mitaka/見たか means "Have you seen it?" in Japanese.