

 **mitre-attack / attack-website**

👁 Watch15

★ Star83

🍴 Fork26

<> Code

🔔 Issues23

🔗 Pull requests0

📁 Projects0

🛡 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

MITRE ATT&CK Website <https://attack.mitre.org>

cybersecurity

mitre-corporation

cyber-threat-intelligence

mitre-attack

cti

📄 98 commits

🌿 8 branches

📦 0 packages

📦 7 releases

👤 3 contributors


📄 Apache-2.0

Branch: master ▾

New pull request

Find file

Clone or download ▾

 **isaisabel** merging develop into master Latest commit cbd9a7f 2 days ago

📁 .github	Add changelog reminder to PR template	12 days ago
📁 attack-theme	removed analytics, fixed some issues with README	12 days ago
📁 content	update roadmap to latest version	5 days ago
📁 data	update ATT&CK content to version 6.2	5 days ago
📁 modules	fixed software sidenav typo	2 days ago
📁 plugins/assets	replace master branch with source code. Static html now found on the ...	16 days ago
📄 .gitignore	replace master branch with source code. Static html now found on the ...	16 days ago
📄 CHANGELOG.md	fixed software sidenav typo	2 days ago
📄 CONTRIBUTING.md	replace master branch with source code. Static html now found on the ...	16 days ago
📄 LICENSE.txt	replace master branch with source code. Static html now found on the ...	16 days ago
📄 NOTICE.txt	replace master branch with source code. Static html now found on the ...	16 days ago
📄 README.md	removed analytics, fixed some issues with README	12 days ago
📄 pelicanconf.py	replace master branch with source code. Static html now found on the ...	16 days ago
📄 requirements.txt	replace master branch with source code. Static html now found on the ...	16 days ago
📄 update-attack.py	replace master branch with source code. Static html now found on the ...	16 days ago

📄 README.md

# MITRE ATT&CK™ Website

See the live site at [attack.mitre.org](https://attack.mitre.org)!

This repository contains the source code used to generate the MITRE ATT&CK™ website as seen at `attack.mitre.org` . The source code is flexible to allow users to generate the site with custom content.

## Usage

The [Install and Run](#) section below explains how to set up a local version of the site. You can also visit the live site at [attack.mitre.org](https://attack.mitre.org). See [Building the site with custom content](#) for information about building the site with custom content.

Use our [Github Issue Tracker](#) to let us know of any bugs or other issues you encounter. We also encourage pull requests if you've extended the site in a cool way and want to share back to the community!

If you find errors or typos in the site content, please let us know by sending an email to [attack@mitre.org](mailto:attack@mitre.org) with the subject **Website Content Error**, and make sure to include both a description of the error and the URL at which it can be found.

See [CONTRIBUTING.md](#) for more information on making contributions to the ATT&CK website.

## Requirements

---

- [python](#) 3.6 or greater

## Install and Build

---

### Install requirements

1. Create a virtual environment:
  - macOS and Linux: `python3 -m venv env`
  - Windows: `py -m venv env`
2. Activate the virtual environment:
  - macOS and Linux: `source env/bin/activate`
  - Windows: `env/Scripts/activate.bat`
3. Install requirement packages: `pip3 install -r requirements.txt`

### Build and serve the local site

1. Update ATT&CK markdown from the STIX content, and generate the output html from the markdown: `python3 update-attack.py -c -b`. *Note: `update-attack.py`, has many optional command line arguments which affect the behavior of the build. Run `python3 update-attack.py -h` for a list of arguments and an explanation of their functionality.*
2. Serve the html to `localhost:8000` :
  - i. `cd output`
  - ii. `python3 -m pelican.server`

## Implementation Overview

---

The ATT&CK site uses a combination of Python, Pelican and Jinja to convert the STIX content into a set of static HTML files. When `update-attack.py` is run, it generates a set of markdown files in `content` containing the parsed STIX content. Pelican then reads these markdown files and uses them to with the Jinja templates in `attack-theme/templates` to build the site HTML in the output directory.

### ATT&CK Archives

The previous-versions feature, built to `/resources/previous-versions/` and `/previous/`, is used to display older versions of the ATT&CK site. This feature is reliant on the [attack-archives](#) repository, which stores the archived versions and also provides the functionality to preserve the current site in the archive. For more information on how the previous-version system works, please see the [attack-archives repository on github](#) or the [archives module](#).

## Building the site with custom content

---

The ATT&CK Website is designed support an evolving knowledge base. The content seen on the site is generated from data in STIX2.0 JSON format. The data used on the live site at [attack.mitre.org](https://attack.mitre.org) can be found on our [mitre/cti](#) github repo.

You can generate the website using custom content by replacing the STIX bundles in `/data/stix/` :

- `enterprise-attack.json` is the bundle for the enterprise domain.
- `mobile-attack.json` is the bundle for the mobile domain.
- `pre-attack.json` is the bundle for the pre-attack domain.

- the `*_old.json` bundles are updated automatically when the site is built, and are used for generating Matrix timestamps. `old_dates.json` is used for fallback timestamps for the matrices. You typically won't need to replace these files.

Users wishing to make changes to the ATT&CK website visual theme should take a look at our scss source files in `attack-theme/static/style`. Changes to the colors defined in `_colors.scss` should automatically propagate across the site. Users wishing to make changes to the layout of pages should modify the templates found in `attack-theme/templates`. Major additions or changes will typically require modification of the python modules in `modules/` in addition to the templates.

## Related MITRE Work

---

### CTI

[Cyber Threat Intelligence repository](#) of the ATT&CK catalog expressed in STIX 2.0 JSON.

### ATT&CK Navigator

The ATT&CK Navigator is an open-source tool providing basic navigation and annotation of ATT&CK matrices, something that people are already doing today in tools like Excel. It is designed to be simple and generic - you can use the Navigator to visualize your defensive coverage, your red/blue team planning, the frequency of detected techniques, and more.

<https://github.com/mitre-attack/attack-navigator>

### STIX

Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI).

STIX enables organizations to share CTI with one another in a consistent and machine readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively.

STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.

<https://oasis-open.github.io/cti-documentation/>

## Notice

---

Copyright 2015-2019 The MITRE Corporation

Approved for Public Release; Distribution Unlimited. Case Number 19-3504.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

This project makes use of ATT&CK™

[ATT&CK Terms of Use](#)