

cisagov/CHIRP: A DFIR tool written in Python.

 github.com/cisagov/CHIRP

cisagov

cisagov/CHIRP

A DFIR tool written in Python.



 4
Contributors

 137
Used by

 1k
Stars

 91
Forks



CHIRP


status **archived** issues **8 open** pull requests **0 open** license **CC0 1.0**










A DFIR tool written in Python.

Watch the [video overview](#)



Table of Contents

-  [Table of Contents](#)

-  [About](#)
-  [Getting Started](#)
 - [Prerequisites](#)
 - [Installing](#)
-  [Usage](#)
-  [Built Using](#)
-  [Authors](#)
-  [Acknowledgements](#)
-  [Contributing](#)
-  [License](#)
-  [Legal Disclaimer](#)

About

The CISA Hunt and Incident Response Program (CHIRP) is a tool created to dynamically query Indicators of Compromise (IoCs) on hosts with a single package, outputting data in a JSON format for further analysis in a SIEM or other tool. CHIRP does not modify any system data.

Getting Started

We build and release CHIRP via [Releases](#). However, if you wish to run with Python3.6+, follow these instructions.

You can also write new [indicators](#) or [plugins](#) for CHIRP.

Prerequisites

Python 3.6 or greater is required to run CHIRP with Python. If you need help installing Python in your environment, follow the instructions [here](#)

CHIRP must be run on a live machine, but it does not have to be network connected.

Installing

```
python3 -m pip install -e .
```

In our experience, yara-python comes with some other dependencies. You MAY have to install Visual Studio C++ 14.0 and the Windows 10 SDK, this can be retrieved with [Visual Studio Community](#)

Usage

From [release](#)

```
# defaults
.\chirp.exe -a AA21-008A

# with args
.\chirp.exe -a AA21-062A -p registry yara -t c:\\target_dir\\** -o chirp_result --
non-interactive -vv
```

From python

```
# defaults
python3 chirp.py -a AA21-008A

# with args
python3 chirp.py -a AA21-062A -p registry yara -t c:\\target_dir\\** -o chirp_result
--non-interactive -vv
```

Example output

```
[15:32:19] [YARA] Enumerating the entire filesystem due to ['CISA Solar Fire', 'CISA
Teardrop', 'CrowdStrike Rempack', 'CrowdStrike Sunspot', 'FireEye          common.py:103
Cosmic Gale', 'FireEye Sunburst']... this is going to take a while.
[YARA] Entered yara plugin.
common.py:103
[REGISTRY] Found 0 hit(s) for IFE0 Persistence indicator.
common.py:103
[REGISTRY] Found 0 hit(s) for Teardrop - Registry Activity indicator.
common.py:103
[REGISTRY] Found 0 hit(s) for Sibot - Registry indicator.
...
...
...
[+] Done! Your results can be found at Z:\README\output.
```

Non-interactive Mode

Non-interactive mode may be used by issuing the "--non-interactive" flag at runtime. Using this flag enables process completion without input. In addition, a non-zero status of 1 will be emitted at runtime completion if IoC's were discovered.

Built Using

- [Python](#) - Language
- [Nuitka](#) - For compilation
- [evtlog2json](#) - For event log access
- [yara-python](#) - Parses and runs yara rules
- [rich](#) - Makes the CLI easier on the eyes
- [psutil](#) - Provides an easy API for many OS functions
- [aiomp](#) - Asynchronous multiprocessing
- [pyyaml](#) - Allows YAML interpretation

Authors

Acknowledgements

- Denise Keating
- Liana Parakesyan
- Richard Kenny
- Megan Nadeau
- Ewa Dadok
- David Zito
- Chris Brown
- Julian Blanco, LTJG USCG
- Caleb Stewart, LT USCG
- James Haughom

Contributing

We welcome contributions! Please see [here](#) for details.

License

This project is in the worldwide public domain.

This project is in the public domain within the United States, and copyright and related rights in the work worldwide are waived through the CC0 1.0 Universal public domain dedication.

All contributions to this project will be released under the CC0 dedication. By submitting a pull request, you are agreeing to comply with this waiver of copyright interest.

Legal Disclaimer

NOTICE

This software package (“software” or “code”) was created by the United States Government and is not subject to copyright within the United States. All other rights are reserved. You may use, modify, or redistribute the code in any manner. However, you may not subsequently copyright the code as it is distributed. The United States Government makes no claim of copyright on the changes you effect, nor will it restrict your distribution of bona fide changes to the software. If you decide to update or redistribute the code, please include this notice with the code. Where relevant, we ask that you credit the Cybersecurity and Infrastructure Security Agency with the following statement: “Original code developed by the Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of Homeland Security.”

USE THIS SOFTWARE AT YOUR OWN RISK. THIS SOFTWARE COMES WITH NO WARRANTY, EITHER EXPRESS OR IMPLIED. THE UNITED STATES GOVERNMENT ASSUMES NO LIABILITY FOR THE USE OR MISUSE OF THIS SOFTWARE OR ITS DERIVATIVES.

THIS SOFTWARE IS OFFERED "AS-IS." THE UNITED STATES GOVERNMENT WILL NOT INSTALL, REMOVE, OPERATE OR SUPPORT THIS SOFTWARE AT YOUR REQUEST. IF YOU ARE UNSURE OF HOW THIS SOFTWARE WILL INTERACT WITH YOUR SYSTEM, DO NOT USE IT.