**Sophos Fakedrop**

Fakedrop is a tool for use with Sophos Intercept X Advanced with EDR to aid with product demonstration and evaluations.

# **Quickstart**

Run Fakedrop in Discovery mode on one computer, and Trigger mode on another computer. Both should be running Sophos Intercept X Advanced with EDR.

A Threat Case will be generated due to the malicious events generated on the Trigger computer by Fakedrop. Artefacts such as low.exe can be used to perform a Threat Search across the estate. This will reveal the events that took place on the Discovery computer.

Threat Intelligence can be gained by submitted the artefacts to SophosLabs within a Threat Case, or a forensic snapshot can be generated and further investigation performed.

With each subsequent execution of the tool, you will be adding to the event data on the endpoint, thus producing a larger graph in the relevant Threat Case. It is best to restart the computer after each use of the tool so that the smallest Threat Case graph is produced.

Fakedrop is designed to look malicious and thus may need to be excluded. The included hashes.txt includes the file hashes for both fakedrop-cli.exe and fakedrop-gui.exe. These can be used to excluded Fakedrop from detection. If fakedrop is detected, follow our documentation to [allow the application](https://docs.sophos.com/central/Customer/help/en-us/central/Customer/concepts/AllowedApplications.html).

# **Overview**

Two builds of the tool are provided. One for use on the command line only (fakedrop-cli.exe / cli.py) and one with a graphical user interface (fakedrop-gui.exe / gui.py). Executables are built using PyInstaller.

Fakedrop has two modes of execution. Discovery mode and Trigger mode.

**Discovery mode**:

* Reads the files in the current working directory.
* Downloads and executes two Sophos test files - unknown.exe and low.exe. These files are benign and are typically used to test Download Reputation.
* Makes HTTP GET requests to two Sophos test webpages on Sophostest.com - one categorized as ‘Criminal Activity’ and one categorized as ‘Downloads’

**Trigger mode**:

* Performs all stages from Discovery mode.
* Downloads and executes two additional, benign, Sophos test files - highscore.exe and sophos\_hips\_test.exe. Highscore.exe is detected by our Deep Learning model as malicious and sophos\_hips\_test.exe is detected by our Host Intrusion Detection System.
* Downloads the EICAR test virus.
* Makes HTTP GET requests to two additional Sophos test webpages on Sophostest.com - one categorized as ‘Call Home / Command and Control’ and one categorized as ‘Malware’.

## Fakedrop-cli.exe

usage: fakedrop-cli.exe [options]

e.g.

fakedrop-cli.exe --accept-eula -d -vvv --skip-hips --logfile C:-log.txt

|  |  |  |
| --- | --- | --- |
| Argument | Description | Required? |
| --accept-eula | Accept the Sophos End User License Agreement and acknowledge the Sophos Privacy Policy | Y |
| -d, --discovery | Drop artefacts without throwing a malicious detection | Y (or -t) |
| -t, --trigger | Drop artefacts and generate a malicious detection | Y (or -d) |
| -v, --verbose | Increase logging output | N |
| -q, --quiet | Decrease logging output | N |
| --skip-hips | Skip the HIPS test file | N |
| --skip-web | Skip HTTP requests to suspicious URLs | N |
| -l, --logfile FILE | Filepath for file to write logging events to | N |
| --version | Print tool version number | N |

## 

## Fakedrop-gui.exe

The GUI offers the same arguments as the CLI version however does so with a tabbed interface.

![Mode selection](data:image/png;base64;base64,)

![Output](data:image/png;base64;base64,)

## Building Fakedrop

Fakedrop is built using [PyInstaller](https://www.pyinstaller.org/). Due to the dependency on [Gooey](https://github.com/chriskiehl/Gooey), it is recommended that you read the [instructions](http://chriskiehl.com/article/packaging-gooey-with-pyinstaller/) published by the Gooey maintainer on how to build with PyInstaller.

## License

Copyright 2018 Sophos Limited

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.