QBOT Configuration Extractor

elastic.co/security-labs/qbot-configuration-extractor

Configuration extraction tool for QBOT malware

By

Elastic Security Labs

27 juillet 2022

Python script to extract the configuration from QBOT samples.

Download qbot-config-extractor.tar.gz

Getting Started

This tool provides a Python module and command line tool that will extract configurations from the QBOT malware samples and dump the results to screen.

The QBOT Attack Pattern

For information on the QBOT attack pattern, check out our blog posts detailing this:

Exploring the QBOT Attack Pattern

Docker

We can easily run the extractor with Docker, first we need to build the image:

```
docker build . -t qbot-config-extractor
```

Then we run the container with the **-v** flag to map a host directory to the docker container directory:

```
docker run -ti --rm -v \
"$(pwd)/data":/data qbot-config-extractor:latest -d /data/
```

We can either specify a single sample with **-f** option or a directory of samples with **-d**.

```
$ docker run -ti --rm -v $(pwd)/data:/data qbot-config-extractor:latest -f
data/c2ba065654f13612ae63bca7f972ea91c6fe97291caeaaa3a28a180fb1912b3a

=== Strings ===
# Blob address: 0x100840a0
# Key address: 0x10084040
[0x0]: ProgramData
[0xc]: /t4
[0x10]: EBBA
[0x15]: netstat -nao
[0x22]: jHxastDcds)oMc=jvh7wdUhxcsdt2
[0x40]: schtasks.exe /Create /RU "NT AUTHORITY\SYSTEM" /SC ONSTART /TN %u /TR "%s"
/NP /F

...truncated...

=== RESOURCE 1 ===
Key: b'\\System32\\WindowsPowerShel1\\v1.0\\powershel1.exe'
Type: DataType.DOMAINS
41.228.22.180:443
47.23.89.62:995
176.67.56.94:443
103.107.113.120:443
148.64.96.100:443
47.180.172.159:443
181.118.183.98:443

...truncated...Read more
```

Running it Locally

As mentioned above, Docker is the recommended approach to running this project, however you can also run this locally. This project uses Poetry to manage dependencies, testing, and metadata. If you have Poetry installed already, from this directory, you can

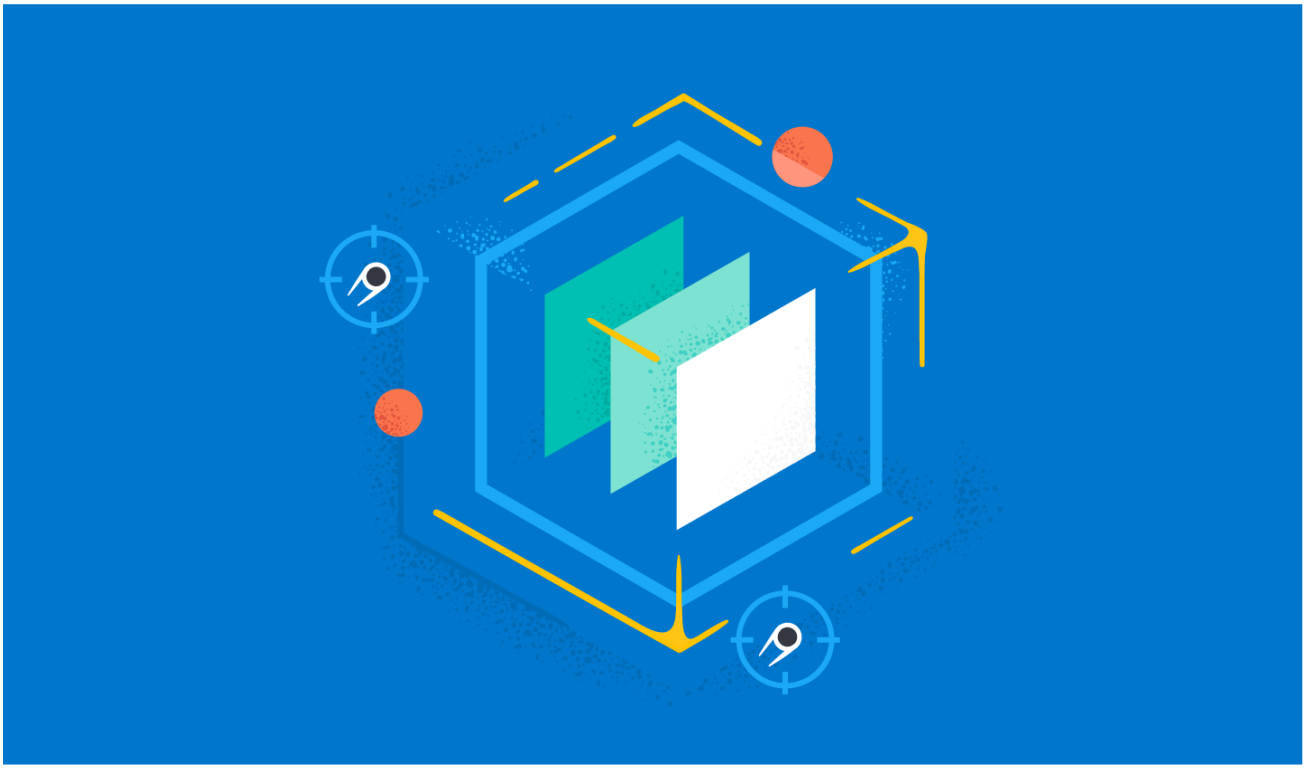
simply run the following commands to run the tool. This will setup a virtual environment, install the dependencies, activate the virtual environment, and run the console script.

```
poetry lock
poetry install
poetry shell
qbot-config-extractor -h
```

Once that works, you can do the same sort of things as mentioned in the Docker instructions above.

Related content

See all top stories

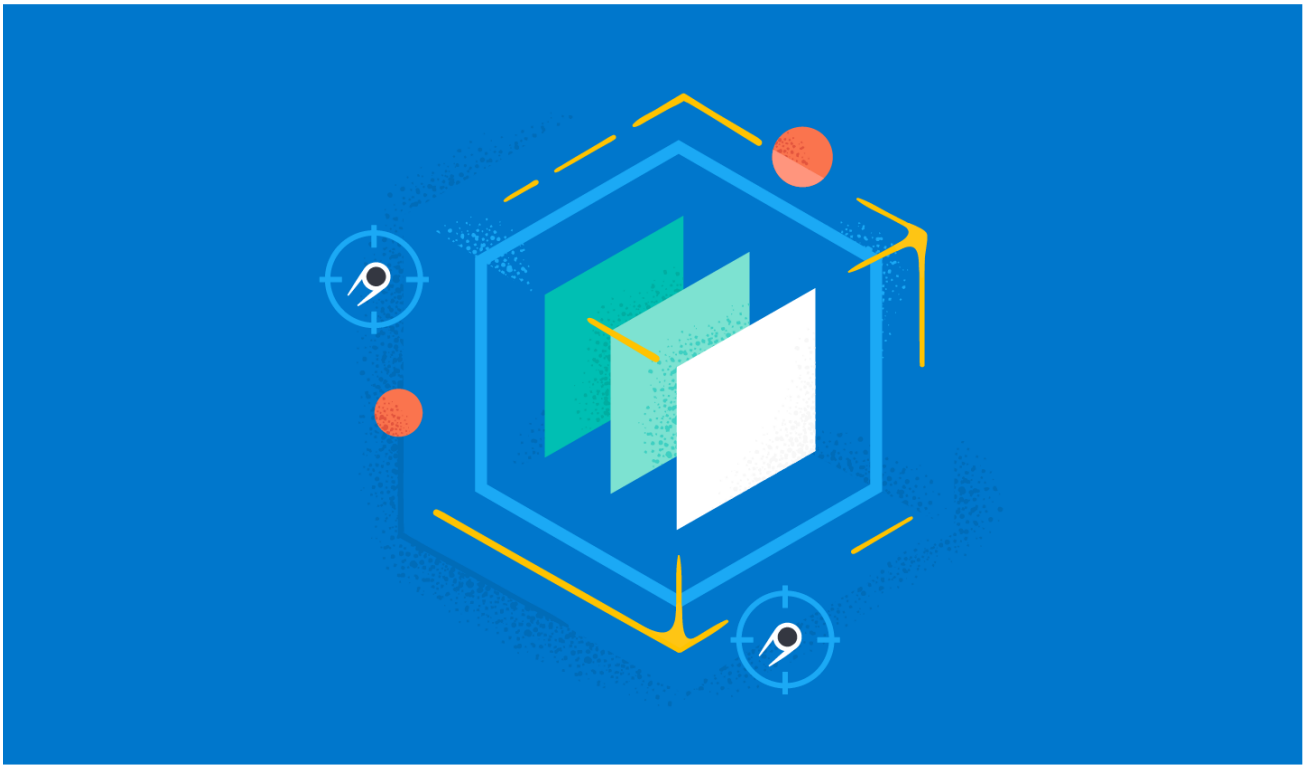


Exploring the QBOT Attack Pattern

In this research publication, we'll explore our analysis of the QBOT attack pattern — a full-featured and prolific malware family.

BLISTER Configuration Extractor

Python script to extract the configuration and payload from BLISTER samples.



BLISTER Loader

The BLISTER loader continues to be actively used to load a variety of malware.