AsyncRAT Configuration Parser

github.com/jeFF0Falltrades/Tutorials/tree/master/asyncrat_config_parser

jeFF0Falltrades

jeFF0Falltrades/
Tutorials

Various Tutorials

1 Contributor | 0 Issues | 32 Stars | 0 Forks

YouTube Video

https://youtu.be/xV0x7kNZ_Yc

YARA Rule for Hunting

https://github.com/jeFF0Falltrades/YARA-Signatures/blob/master/Broadbased/asyncrat.yar

Requirements

```
pip install cryptography
```

or

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

Usage

```
usage: asyncrat_config_parser.py [-h] [-d] file_paths [file_paths ...]

positional arguments:
  file_paths   One or more AsyncRAT payload file paths (deobfuscated)

optional arguments:
  -h, --help   show this help message and exit
  -d, --debug  Enable debug logging
```

Example Input/Output

```
$ python3 asyncrat_config_parser.py ReverseMe.exe | python -m json.tool
{
    "aes_key": "40766aef6f9d6980c001babeef7020446eff2ef31cf910cab59d5429d7a89c37",
    "aes_salt": "bfeb1e56fbcd973bb219022430a57843003d5644d21e62b9d4f180e7e6c33941",
    "config": {
        "Anti": "false",
        "BDOS": "false",
        "Certificate":
"MIIE8jCCAtqgAwIBAgIQAMe2UpmBbjqdMItW7xySBzANBgkqhkiG9w0BAQ0FADAaMRgwFgYDVQQDDA9Bc3luY

        "Delay": "3",
        "Group": "Default",
        "Hosts": "test.me.com",
        "Install": "false",
        "InstallFile": "",
        "InstallFolder": "%AppData%",
        "Key": "N3UwelhLaE5BaTE5Z3piMFEwMFZlWHI2Z01Nc3dPOWM=",
        "MTX": "AsyncMutex_6SI8OkPnk",
        "Pastebin": "null",
        "Ports": "8808,7707",
        "Serversignature":
"ZKSsdlzb5lEwgaF35KH+qv8Ai7M74R+W9CU2NpGy4ucvLuKhDbUpJtqllJuFAk22wP6qgCQ8lvE8zy+LlVHmC

        "Version": "0.5.7B"
    },
    "file_path": "ReverseMe.exe"
}
```