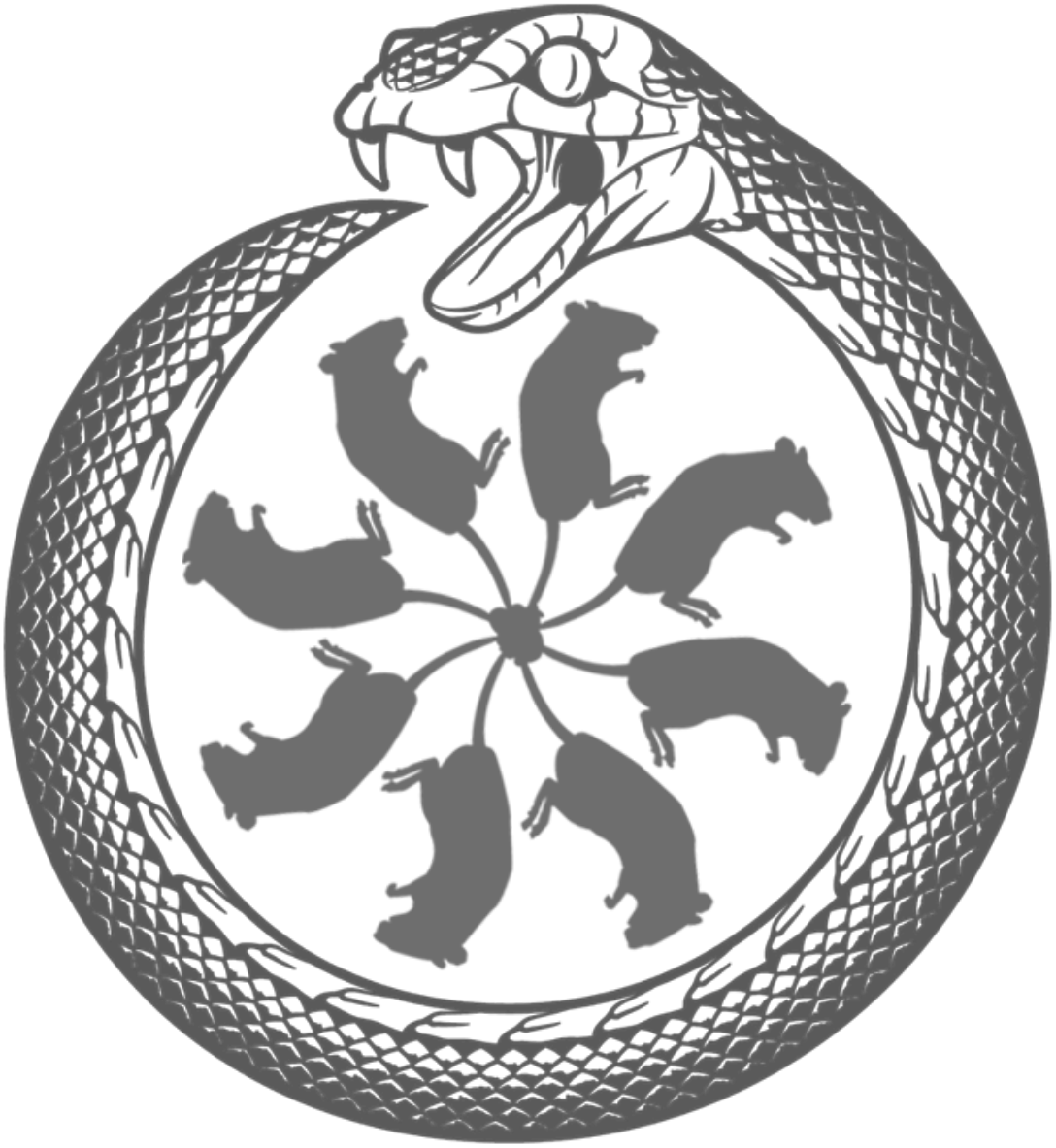
GitHub - jeFF0Falltrades/rat_king_parser: A robust, multiprocessing-capable, multi-family RAT config parser/config extractor for AsyncRAT, DcRAT, VenomRAT, QuasarRAT, XWorm, Xeno RAT, and cloned/derivative RAT families.

By jeFF0Falltrades

Archived: 2026-04-05 14:11:06 UTC



The RAT King Parser

A robust, multiprocessing-capable, multi-family RAT config parser/extractor, tested for use with:

- AsyncRAT
- DcRAT
- VenomRAT
- QuasarRAT
- XWorm
- XenoRat
- Other cloned/derivative RAT families of the above

This configuration parser seeks to be "robust" in that it does not require the user to know anything about the strain or configuration of the RAT ahead of time:

It looks for common configuration patterns present in the above-mentioned RAT families (as well as several clones and derivatives), parses and decrypts the configuration section, using brute-force if simpler patterns are not found, and uses YARA to suggest a possible family for the payload.

The original (much less robust) version of this parser is detailed in the accompanying YouTube code overview video here:

- https://www.youtube.com/watch?v=yoz44QKe_2o

and based on the original AsyncRAT config parser and tutorial here:

- https://github.com/jeFF0Falltrades/Tutorials/tree/master/asyncrat_config_parser

Usage

Installation

As of `v3.1.2`, the RAT King Parser is now available on PyPI and can be installed via `pip`:

```
pip install rat-king-parser
```

Note that YARA must be installed separately.

Usage Help

```
 $ rat-king-parser -h
usage: rat-king-parser [-h] [-v] [-d] [-n] [-p] [-r] [-y YARA] file_paths [file_paths ...]

positional arguments:
  file_paths           One or more RAT payload file paths
```

```
options:
  -h, --help           show this help message and exit
  -v, --version        show program's version number and exit
  -d, --debug          Enable debug logging
  -n, --normalize      Attempt to translate common variations of config keys to normalized field names
  -p, --preserve-keys  Preserve potentially obfuscated configuration keys as-is instead of replacing them with p
  -r, --recompile      Recompile the YARA rule file used for family detection prior to running the parser
  -y, --yara YARA  Uses the *compiled* yara rule at this path to determine the potential family of each payload
```

Using YARA for Payload Identification

A YARA rule for RAT family identification is included with this script in `yara_utils` in both raw and compiled forms.

However, using the `--yara` flag allows a user to specify their own custom YARA rule (in compiled form) to use for identification as well.

If you encounter errors using the included compiled YARA rule (which most often occur due to mismatched YARA versions), the included rule can be recompiled using your local YARA version by specifying the `--recompile` flag.

`yara_utils/recompile.py`, which is the script invoked by the `--recompile` flag, can also be executed on its own to (re)compile any YARA rule:

```
 $ python yara_utils/recompile.py -h
usage: recompile.py [-h] [-i INPUT] [-o OUTPUT]

options:
  -h, --help            show this help message and exit
  -i INPUT, --input INPUT
                        YARA rule to compile
  -o OUTPUT, --output OUTPUT
                        Compiled rule output path
```

```
python recompile.py -i my_rule.yar -o my_rule.yarc
```

External Integrations

As of `v3.1.0`, RAT King Parser has introduced additional, optional wrapper extractors for integration with some external services.

These currently include:

- MACO: The Canadian Centre for Cyber Security's malware config extractor framework, which allows RAT King Parser to be integrated with MACO-compatible tools like AssemblyLine (though RAT King

Parser is already integrated in AssemblyLine's configuration extraction service without need for further configuration)

In order to utilize these extractors, the optional dependencies for a particular extractor must be installed.

This can be completed with `pip` by referencing the specific optional dependency group to install; For example:

```
pip install "rat_king_parser[maco] @ git+https://github.com/jeFF0Falltrades/rat_king_parser.git"
```

Example Input/Output

Not Preserving Obfuscated Keys

```
$ rat-king-parser -n dangerzone/* | jq
```


```
[
  {
    "file_path": "dangerzone/034941c1ea1b1ae32a653aab6371f760dfc4fc43db7c7bf07ac10fc9e98c849e",
    "sha256": "034941c1ea1b1ae32a653aab6371f760dfc4fc43db7c7bf07ac10fc9e98c849e",
    "yara_possible_family": "dcrat",
    "key": "3915b12d862a41cce3da2e11ca8cefc26116d0741c23c0748618add80ee31a5c",
    "salt": "4463526174427971777164616e6368756e",
    "config": {
      "Ports": [
        "2525"
      ],
      "Hosts": [
        "20.200.63.2"
      ],
      "Version": " 1.0.7",
      "Install": "false",
      "InstallFolder": "%AppData%",
      "InstallFile": "",
      "Key": "dU81ekM1S2pQYmVOWWhQcjV4WlJwcWRkSnVYR2tTQ0w=",
      "Mutex": "DcRatMutex_qwqdanchun",
      "Certificate": "MIICMDCCAZmgAwIBAgIVANpXtGwt9qBbU/pdFz8d/Pt6kzb7MA0GCSqGSIb3DQEBDQUAMGQxFTATBg
      "Serversignature": "c+KGE0Aw1XRgjGe2Kvay1H3VgUgqKRYGit46DnCR6eW/g+kO+H5oRsfBNkVizj0Q862zTXvLkW
      "Pastebin": "null",
      "BSOD": "false",
      "Hwid": "null",
      "Delay": "1",
      "Group": "16JUNIO-PJOAO",
      "AntiProcess": "false",
      "Anti": "false"
    }
```

```
  },
  {
    "file_path": "dangerzone/0aa7bfb081e73a67c23715a55ff13a74ef6b1ce2b82a33b5537ee001592919a4",
    "sha256": "0aa7bfb081e73a67c23715a55ff13a74ef6b1ce2b82a33b5537ee001592919a4",
    "yara_possible_family": "asyncrat",
    "key": "564eced38c73ee8089d8bcc951f28c0589a54388a4058b0da1d9c4d94514518f",
    "salt": "bfeb1e56fbcd973bb219022430a57843003d5644d21e62b9d4f180e7e6c33941",
    "config": {
      "TelegramToken": "7153134069:AAHd4riTPdhAdVGBwo16vJQ5H3eORu5QAEo",
      "TelegramChatID": "1863892139",
      "Ports": [
        "6606",
        "7707",
        "8808"
      ],
      "Hosts": [
        "127.0.0.1"
      ],
      "Version": "",
      "Install": "false",
      "InstallFolder": "%AppData%",
      "InstallFile": "",
      "Key": "Uk9tU0hKZUlVdXBwek1tV3NqYnBLYVRYcklWQXB5c0I=",
      "Mutex": "AsyncMutex_6SI8OkPnk",
      "Certificate": "MIIE9jCCAt6gAwIBAgIQAKQXqY8ZdB/modqi69mWGTANBgkqhkiG9w0BAQ0FADAcMRowGAYDVQQDDB
      "Serversignature": "b4TmzraaQMXPVpdfH6wgqDtnXhWP9SP6GdUMgvKSpjPlWufiGM88XWg3Wnv1bduWRMUOAIBN31
      "Anti": "false",
      "Pastebin": "null",
      "BDOS": "false",
      "Hwid": "null",
      "Delay": "3",
      "Group": "Default"
    }
  },
  {
    "file_path": "dangerzone/0e19cefba973323c234322452dfd04e318f14809375090b4f6ab39282f6ba07e",
    "sha256": "0e19cefba973323c234322452dfd04e318f14809375090b4f6ab39282f6ba07e",
    "yara_possible_family": "asyncrat",
    "key": "None",
    "salt": "bfeb1e56fbcd973bb219022430a57843003d5644d21e62b9d4f180e7e6c33941",
    "config": {
      "Ports": [
        "%Ports%"
      ],
      "Hosts": [
        "%Hosts%"
      ],
```

```
      "Version": "%Version%",
      "Install": "%Install%",
      "InstallFolder": "%Folder%",
      "InstallFile": "%File%",
      "Key": "%Key%",
      "Mutex": "%MTX%",
      "Certificate": "%Certificate%",
      "Serversignature": "%Serversignature%",
      "Anti": "%Anti%",
      "Pastebin": "%Pastebin%",
      "BDOS": "%BDOS%",
      "Hwid": "null",
      "Delay": "%Delay%",
      "Group": "%Group%"
    }
  },
  {
    "file_path": "dangerzone/6b99acfa5961591c39b3f889cf29970c1dd48ddb0e274f14317940cf279a4412",
    "sha256": "6b99acfa5961591c39b3f889cf29970c1dd48ddb0e274f14317940cf279a4412",
    "yara_possible_family": "asyncrat",
    "key": "eebdb6b2b00c2501b7b246442a354c5c3d743346e4cc88896ce68485dd6bbb8f",
    "salt": "bfeb1e56fbcd973bb219022430a57843003d5644d21e62b9d4f180e7e6c33941",
    "config": {
      "Ports": [
        "2400"
      ],
      "Hosts": [
        "minecraftdayzserver.ddns.net"
      ],
      "Version": "0.5.8",
      "Install": "true",
      "InstallFolder": "%AppData%",
      "InstallFile": "WinRar.exe",
      "Key": "VUpkMU9UTEhRSEVSN2d2eWpLeDJud2Q0STFIcDRXS0U=",
      "Mutex": "LMAsmxp3mz2D",
      "Certificate": "MIIE4DCCAsigAwIBAgIQAM+WaL4OeJIj4I0Usukl1TANBgkqhkiG9w0BAQ0FADARMQ8wDQYDVQQDDA
      "Serversignature": "PBjqcvsYypDmnjgUVv1SkvtLx+jFt2V7NyZ+nHik0CWcLbwOwBXD6/3an89d/I7pFAxwZXgSiL
      "Anti": "false",
      "Pastebin": "null",
      "BDOS": "false",
      "Hwid": "null",
      "Delay": "3",
      "Group": "Default"
    }
  },
  {
    "file_path": "dangerzone/83892117f96867db66c1e6676822a4c0d6691cde60449ee47457f4cc31410fce",
```

```
    "sha256": "83892117f96867db66c1e6676822a4c0d6691cde60449ee47457f4cc31410fce",
    "yara_possible_family": "quasarrat",
    "key": "ff230bfb57fecad4bd59d4d97f6883b4",
    "salt": "bfeb1e56fbcd973bb219022430a57843003d5644d21e62b9d4f180e7e6c33941",
    "config": {
      "obfuscated_key_1": "1.3.0.0",
      "obfuscated_key_2": "qztadmin.duckdns.org:9782;",
      "obfuscated_key_3": 3000,
      "obfuscated_key_4": "1WvgEMPjdwfqIMeM9MclyQ==",
      "obfuscated_key_5": "NcFtjbDOcsw7Evd3coMC0y4koy/SRZGydhNmno81ZOWOvdfg7sv0Cj5ad2ROUfX4QMscAIjYJ
      "obfuscated_key_6": "APPLICATIONDATA",
      "obfuscated_key_7": "SubDir",
      "obfuscated_key_8": "Client.exe",
      "obfuscated_key_9": false,
      "obfuscated_key_10": false,
      "obfuscated_key_11": "QSR_MUTEX_YMblzlA3rm38L7nnxQ",
      "obfuscated_key_12": "Quasar Client Startup",
      "obfuscated_key_13": false,
      "obfuscated_key_14": true,
      "obfuscated_key_15": "mDf8ODHd9XwqMsIxpY8F",
      "obfuscated_key_16": "Office04",
      "obfuscated_key_17": "Logs",
      "obfuscated_key_18": true,
      "obfuscated_key_19": false
    }
  },
  {
    "file_path": "dangerzone/9bfed30be017e62e482a8792fb643a0ca4fa22167e4b239cde37b70db241f2c4",
    "sha256": "9bfed30be017e62e482a8792fb643a0ca4fa22167e4b239cde37b70db241f2c4",
    "yara_possible_family": "venomrat",
    "key": "86cfd98ca989924e7a9439902dc6a72e315da09c11b100c39cd59b9c9372b192",
    "salt": "56656e6f6d524154427956656e6f6d",
    "config": {
      "Ports": [
        "4449"
      ],
      "Hosts": [
        "127.0.0.1"
      ],
      "Version": "Venom RAT + HVNC + Stealer + Grabber  v6.0.3",
      "Install": "false",
      "InstallFolder": "%AppData%",
      "InstallFile": "speedy",
      "Key": "TzY1S0thald3UGNURmJTYjNSQVdBYlBQR2tTdUFaTTg=",
      "Mutex": "ypxcfziuep",
      "Certificate": "MIICNjCCAZ+gAwIBAgIVALWZXeRliC16frxuoSrGsVJO4U2tMA0GCSqGSIb3DQEBDQUAMGcxFTATBg
      "Serversignature": "Sn1WeJuN+Ypb6kUw4QirT1RzbwUEoeSYTmJAIlg0LayMd/VSwAo+0LnnT/g5HFx4QrqaM689Cv
```

```
      "Pastebin": "null",
      "BSOD": "false",
      "Hwid": "null",
      "Delay": "1",
      "Group": "Default",
      "AntiProcess": "false",
      "Anti": "true"
    }
  },
  {
    "file_path": "dangerzone/a2817702fecb280069f0723cd2d0bfdca63763b9cdc833941c4f33bbe383d93e",
    "sha256": "a2817702fecb280069f0723cd2d0bfdca63763b9cdc833941c4f33bbe383d93e",
    "yara_possible_family": "quasarrat",
    "key": "None",
    "salt": "None",
    "config": {
      "Version": "1.0.00.r3",
      "RECONNECTDELAY": 5000,
      "PASSWORD": "5EPmsqV4iTCGjx9aY3yYpBWD0IgEJpHNEP75pks",
      "SPECIALFOLDER": "APPLICATIONDATA",
      "SUBFOLDER": "SUB",
      "INSTALLNAME": "INSTALL",
      "INSTALL": false,
      "STARTUP": true,
      "Mutex": "e4d6a6ec-320d-48ee-b6b2-fa24f03760d4",
      "STARTUPKEY": "STARTUP",
      "HIDEFILE": true,
      "ENABLELOGGER": true,
      "Key": "O2CCRlKB5V3AWlrHVKWMrr1GvKqVxXWdcx0l0s6L8fB2mavMqr",
      "Group": "RELEASE",
      "hardcoded_hosts": [
        "kilofrngcida.xyz:443",
        "sartelloil.lat:443",
        "fostlivedol.xyz:443",
        "comerciodepeixekino.org:443",
        "cartlinkfoltrem.xyz:443",
        "trucks-transport.xyz:443"
      ]
    }
  },
  {
    "file_path": "dangerzone/a76af3d67a95a22efd83d016c9142b7ac9974068625516de23e77a5ac3dd051b",
    "sha256": "a76af3d67a95a22efd83d016c9142b7ac9974068625516de23e77a5ac3dd051b",
    "yara_possible_family": "quasarrat",
    "key": "b30cea630f7fac6c2e066ce7f29e1b4bab548ee95b20ff6aa7387ce14df5dc30",
    "salt": "bfeb1e56fbcd973bb219022430a57843003d5644d21e62b9d4f180e7e6c33941",
    "config": {
```

```
      "obfuscated_key_1": "1.4.1",
      "obfuscated_key_2": "10.0.0.61:4782;24.67.68.3:4782;",
      "obfuscated_key_3": 3000,
      "obfuscated_key_4": "APPLICATIONDATA",
      "obfuscated_key_5": "SubDir",
      "obfuscated_key_6": "GloomTool.exe",
      "obfuscated_key_7": true,
      "obfuscated_key_8": true,
      "obfuscated_key_9": "9fdd3e80-d560-431b-b526-3ebbc1799110",
      "obfuscated_key_10": "WindowsAV",
      "obfuscated_key_11": true,
      "obfuscated_key_12": true,
      "obfuscated_key_13": "5F91B88C67A9ACF78B2396771B3B6F2B4615CA57",
      "obfuscated_key_14": "Office04",
      "obfuscated_key_15": "Logs",
      "obfuscated_key_16": "KQrwmpZSwOF20ZdNZlVJ7YjgErzUf9cophPOCAULRI4gSid7qeSaRL4LhhUXzEq1JuUlkRR7
      "obfuscated_key_17": "MIIE9DCCAtygAwIBAgIQAIhqXB+nLwd+VvEk3rjLsTANBgkqhkiG9w0BAQ0FADAbMRkwFwYD
      "obfuscated_key_18": true,
      "obfuscated_key_19": true,
      "obfuscated_key_20": "",
      "obfuscated_key_21": "",
      "obfuscated_key_22": true
    }
  },
  {
    "file_path": "dangerzone/b5bff486f091f9539606931e0aff280eaea17064b2a12940675dfac926e9666e.exe",
    "sha256": "b5bff486f091f9539606931e0aff280eaea17064b2a12940675dfac926e9666e",
    "yara_possible_family": "xworm",
    "key": "c527ac2a4eeb6039d9477583d0f4f2c527ac2a4eeb6039d9477583d0f4f2ee00",
    "salt": "None",
    "config": {
      "Hosts": [
        "act-cleaning.gl.at.ply.gg"
      ],
      "Ports": [
        "37158"
      ],
      "KEY": "<123456789>",
      "SPL": "<Xwormmm>",
      "Sleep": 3,
      "Group": "NeverLoseCrack",
      "USBNM": "USB.exe",
      "InstallDir": "%ProgramData%",
      "InstallStr": "svchost.exe",
      "Mutex": "OkWVOTioL6k3Fg3w",
      "LoggerPath": "\\Log.tmp"
    }
```

```
  },
  {
    "file_path": "dangerzone/beb1b5cd2a33e86e48599b183b882fc3e80198a8062e5b9d9251e605d3f0bfd5.exe",
    "sha256": "beb1b5cd2a33e86e48599b183b882fc3e80198a8062e5b9d9251e605d3f0bfd5",
    "yara_possible_family": "quasarrat",
    "key": "b5580a84ddadcf548713dd64fedbbe067f931e6ce4699271de572acbd52f4074",
    "salt": "bfeb1e56fbcd973bb219022430a57843003d5644d21e62b9d4f180e7e6c33941",
    "config": {
      "obfuscated_key_1": "1.4.1",
      "obfuscated_key_2": "91.92.241.122:6969;",
      "obfuscated_key_3": 3000,
      "obfuscated_key_4": "APPLICATIONDATA",
      "obfuscated_key_5": "",
      "obfuscated_key_6": "Client.exe",
      "obfuscated_key_7": true,
      "obfuscated_key_8": true,
      "obfuscated_key_9": "fcf2be0a-a426-40c6-b153-1a354814f80d",
      "obfuscated_key_10": "Quasar Client Startup",
      "obfuscated_key_11": false,
      "obfuscated_key_12": true,
      "obfuscated_key_13": "26A6C07FE7354BCD244B108D2E3538DCF04477F5",
      "obfuscated_key_14": "Fab",
      "obfuscated_key_15": "Logs",
      "obfuscated_key_16": "U/jVlmjpH/9zMrLFla8LcLavxUQe9wt9L6qGAh9zYqPdqDW0e0fRlnxEST/s3HTVlAyuqIyn
      "obfuscated_key_17": "MIIE9DCCAtygAwIBAgIQAJMC1KOnf3PAJ47sO2MclTANBgkqhkiG9w0BAQ0FADAbMRkwFwYD
      "obfuscated_key_18": false,
      "obfuscated_key_19": false,
      "obfuscated_key_20": "",
      "obfuscated_key_21": "",
      "obfuscated_key_22": true
    }
  },
  {
    "file_path": "dangerzone/d5028e10a756f2df677f32ebde105d7de8df37e253c431837c8f810260f4428e",
    "sha256": "d5028e10a756f2df677f32ebde105d7de8df37e253c431837c8f810260f4428e",
    "yara_possible_family": "xenorat",
    "key": "650f47cdd14eaef8c529f2a03fa7744c",
    "salt": "None",
    "config": {
      "Hosts": [
        "77.221.152.198"
      ],
      "Ports": 4444,
      "Key": "03ac674216f3e15c761ee1a5e255f067953623c8b388b4459e13f978d7c846f4",
      "delay": 5000,
      "mutexstring": "Xeno_rat_nd89dsedwqdswdqwdwqdqwdqwdwqdwqdqwdqwdwqdwqd12d",
      "DoStartup": 2222,
```

```
      "Installpath": "appdata",
      "startupname": "nothingset"
    }
  },
  {
    "file_path": "dangerzone/db09db5bdf1dcf6e607936a6abbe5ce91efbbf9ce136efc3bdb45222710792fa",
    "sha256": "db09db5bdf1dcf6e607936a6abbe5ce91efbbf9ce136efc3bdb45222710792fa",
    "yara_possible_family": "venomrat",
    "key": "11ed70df5ce22de750c6e7496fa5c51985c321d2d9dd463979337af003644f41",
    "salt": "56656e6f6d524154427956656e6f6d",
    "config": {
      "Ports": [
        "4449",
        "7772"
      ],
      "Hosts": [
        "127.0.0.1"
      ],
      "Version": "Venom RAT + HVNC + Stealer + Grabber  v6.0.3",
      "Install": "false",
      "InstallFolder": "%AppData%",
      "InstallFile": "",
      "Key": "M1NoWkREazBvNTNGUkRlT0s4TjE1QlRRQmx4bW1zd2U=",
      "Mutex": "qmhvogiycvwh",
      "Certificate": "MIICOTCCAaKgAwIBAgIVAPyfwFFMs6hxoSr1U5gHJmBruaj1MA0GCSqGSIb3DQEBDQUAMGoxGDAWBg
      "Serversignature": "BW9mNNWdLZ+UgmfSTOot753DE24GfE+H6HYG5yl4IFszdMLpfQXijxVlt3bcz68PrHwYG2R70J
      "Pastebin": "null",
      "BSOD": "false",
      "Hwid": "null",
      "Delay": "1",
      "Group": "Default",
      "AntiProcess": "false",
      "Anti": "false"
    }
  },
  {
    "file_path": "dangerzone/fb0d45b0e48b0cdda2dd8c5a152f3c7a375c18d63e588f6a217c9d47f7d5199d",
    "sha256": "fb0d45b0e48b0cdda2dd8c5a152f3c7a375c18d63e588f6a217c9d47f7d5199d",
    "yara_possible_family": "xworm",
    "key": "e5f7efe2fddd6755c92cbc39d5559ce5f7efe2fddd6755c92cbc39d5559c4000",
    "salt": "None",
    "config": {
      "obfuscated_key_1": "mo1010.duckdns.org",
      "obfuscated_key_2": "7000",
      "obfuscated_key_3": "<123456789>",
      "obfuscated_key_4": "<Xwormmm>",
      "obfuscated_key_5": 3,
```

```
      "obfuscated_key_6": "USB.exe",
      "obfuscated_key_7": "%AppData%",
      "obfuscated_key_8": "tBZ7NDtphvUCm0Dc",
      "obfuscated_key_9": "\\Log.tmp"
    }
  },
  {
    "file_path": "dangerzone/vstdlib_s64",
    "sha256": "6e5671dec52db7f64557ba8ef70caf53cf0c782795236b03655623640f9e6a83",
    "yara_possible_family": "quasarrat",
    "key": "526f35346a62726168486530765a6266487a703968557552663768 4a737575794b4c7933654e5a3465644c41
    "salt": "None",
    "config": {
      "Version": "1.0.00.r6",
      "RECONNECTDELAY": 5000,
      "PASSWORD": "5EPmsqV4iTCGjx9aY3yYpBWD0IgEJpHNEP75pks",
      "SPECIALFOLDER": "APPLICATIONDATA",
      "SUBFOLDER": "SUB",
      "INSTALLNAME": "INSTALL",
      "INSTALL": false,
      "STARTUP": true,
      "Mutex": "e4d6a6ec-320d-48ee-b6b2-fa24f03760d4",
      "STARTUPKEY": "STARTUP",
      "HIDEFILE": true,
      "ENABLELOGGER": true,
      "Key": "O2CCRlKB5V3AWlrHVKWMrr1GvKqVxXWdcx0l0s6L8fB2mavMqr",
      "Group": "RELEASE",
      "xor_decoded_strings": [
        "BPN - Nuestro Banco",
        "Red Link - bpn",
        "HB Judiciales BPN",
        "Ingresá a tu cuenta",
        "Online Banking Web",
        "Banca Empresa 3.0",
        "Banco Ciudad",
        "Banco Ciudad | Autogestión",
        "Banca Empresa 3.0",
        "Banco Comafi - Online Banking",
        "Banco Comafi - eBanking Empresas",
        "Online Banking Santander | Inicio de Sesión",
        "Online Banking Empresas",
        "Online Banking",
        "Office Banking",
        "HSBC Argentina",
        "HSBC Argentina | Bienvenido",
        "accessbanking.com.ar/RetailHomeBankingWeb/init.do?a=b",
        "ICBC Access Banking | Home Banking",
```

```
        "Banco Patagonia",
        "ebankpersonas.bancopatagonia.com.ar/eBanking/usuarios/login.htm",
        "Página del Banco de la Provincia de Buenos Aires",
        "Red Link",
        "bind - finanzas felices :)",
        "BindID Ingreso",
        "BBVA Net Cash | Empresas | BBVA Argentina",
        "Bienvenido a nuestra Banca Online | BBVA Argentina",
        "Ingresá tu e-mail, teléfono o usuario de Mercado Pago",
        "Mercado Pago | De ahora en adelante, hacés más con tu dinero.",
        "Mercado Pago",
        "Home Banking",
        "Office Banking",
        "Banco Santa Cruz Gobierno - Una propuesta para cada Comuna o Municipio | Banco Santa Cruz",
        "Home banking",
        "Office Banking",
        "Banco de Santa Cruz",
        "Red Link",
        "Banco de la Nación Argentina",
        "Red Link - BANCO DE LA NACION ARGENTINA",
        "Red Link",
        "Macro | Agenda powered by Whyline",
        "Banco Macro | Banca Internet Personas",
        "Banco Macro | NUEVA Banca Internet Empresas",
        "https://argentina-e4162-default-rtdb.firebaseio.com/user.json",
        "C:\\\\Users\\\\",
        "\\\\AppData\\\\Local\\\\Aplicativo Itau",
        "C:\\\\Program Files\\\\Topaz OFD\\\\Warsaw",
        "C:\\\\ProgramData\\\\scpbrad",
        "C:\\\\ProgramData\\\\Trusteer",
        "dd.MM.yyyy HH:mm:ss",
        "application/json",
        "Sistema no disponible, intente nuevamente más tarde.",
        "SENHA DE 6 BPN",
        "SENHA DE 6 NB",
        "SENHA DE 6 CIUDAD",
        "SENHA DE 6 COMAFI",
        "SENHA DE 6 GALACIA",
        "SENHA DE 6 HSBC",
        "SENHA DE 6 ICBC",
        "SENHA DE 6 PATAGONIA",
        "SENHA DE 6 PROVINCIA",
        "SENHA DE 6 SANTANDER",
        "SENHA DE 6 BIND",
        "SENHA DE 6 BBVA",
        "driftcar.giize.com:443",
        "adreniz.kozow.com:443"
```

```
      ]
    }
  }
]
```

Preserving Obfuscated Keys

```
$ rat-king-parser -np dangerzone/* | jq
```


```
[
  {
    "file_path": "dangerzone/034941c1ea1b1ae32a653aab6371f760dfc4fc43db7c7bf07ac10fc9e98c849e",
    "sha256": "034941c1ea1b1ae32a653aab6371f760dfc4fc43db7c7bf07ac10fc9e98c849e",
    "yara_possible_family": "dcrat",
    "key": "3915b12d862a41cce3da2e11ca8cefc26116d0741c23c0748618add80ee31a5c",
    "salt": "4463526174427971777164616e6368756e",
    "config": {
      "Ports": [
        "2525"
      ],
      "Hosts": [
        "20.200.63.2"
      ],
      "Version": " 1.0.7",
      "In_stall": "false",
      "Install_Folder": "%AppData%",
      "Install_File": "",
      "Key": "dU81ekM1S2pQYmVOWWhQcjV4WlJwcWRkSnVYR2tTQ0w=",
      "Mutex": "DcRatMutex_qwqdanchun",
      "Certifi_cate": "MIICMDCCAZmgAwIBAgIVANpXtGwt9qBbU/pdFz8d/Pt6kzb7MA0GCSqGSIb3DQEBDQUAMGQxFTATB
      "Server_signa_ture": "c+KGE0Aw1XRgjGe2Kvay1H3VgUgqKRYGit46DnCR6eW/g+kO+H5oRsfBNkVizj0Q862zTXvL
      "Paste_bin": "null",
      "BS_OD": "false",
      "Hw_id": "null",
      "De_lay": "1",
      "Group": "16JUNIO-PJOAO",
      "Anti_Process": "false",
      "An_ti": "false"
    }
  },
  {
    "file_path": "dangerzone/0aa7bfb081e73a67c23715a55ff13a74ef6b1ce2b82a33b5537ee001592919a4",
    "sha256": "0aa7bfb081e73a67c23715a55ff13a74ef6b1ce2b82a33b5537ee001592919a4",
    "yara_possible_family": "asyncrat",
    "key": "564eced38c73ee8089d8bcc951f28c0589a54388a4058b0da1d9c4d94514518f",
```

```
    "salt": "bfeb1e56fbcd973bb219022430a57843003d5644d21e62b9d4f180e7e6c33941",
    "config": {
      "TelegramToken": "7153134069:AAHd4riTPdhAdVGBwo16vJQ5H3eORu5QAEo",
      "TelegramChatID": "1863892139",
      "Ports": [
        "6606",
        "7707",
        "8808"
      ],
      "Hosts": [
        "127.0.0.1"
      ],
      "Version": "",
      "Install": "false",
      "InstallFolder": "%AppData%",
      "InstallFile": "",
      "Key": "Uk9tU0hKZUlVdXBwek1tV3NqYnBLYVRYcklWQXB5c0I=",
      "Mutex": "AsyncMutex_6SI8OkPnk",
      "Certificate": "MIIE9jCCAt6gAwIBAgIQAKQXqY8ZdB/modqi69mWGTANBgkqhkiG9w0BAQ0FADAcMRowGAYDVQQDDB
      "Serversignature": "b4TmzraaQMXPVpdfH6wgqDtnXhWP9SP6GdUMgvKSpjPlWufiGM88XWg3Wnv1bduWRMUOAIBN31
      "Anti": "false",
      "Pastebin": "null",
      "BDOS": "false",
      "Hwid": "null",
      "Delay": "3",
      "Group": "Default"
    }
  },
  {
    "file_path": "dangerzone/0e19cefba973323c234322452dfd04e318f14809375090b4f6ab39282f6ba07e",
    "sha256": "0e19cefba973323c234322452dfd04e318f14809375090b4f6ab39282f6ba07e",
    "yara_possible_family": "asyncrat",
    "key": "None",
    "salt": "bfeb1e56fbcd973bb219022430a57843003d5644d21e62b9d4f180e7e6c33941",
    "config": {
      "Ports": [
        "%Ports%"
      ],
      "Hosts": [
        "%Hosts%"
      ],
      "Version": "%Version%",
      "Install": "%Install%",
      "InstallFolder": "%Folder%",
      "InstallFile": "%File%",
      "Key": "%Key%",
      "Mutex": "%MTX%",
```

```
      "Certificate": "%Certificate%",
      "Serversignature": "%Serversignature%",
      "Anti": "%Anti%",
      "Pastebin": "%Pastebin%",
      "BDOS": "%BDOS%",
      "Hwid": "null",
      "Delay": "%Delay%",
      "Group": "%Group%"
    }
  },
  {
    "file_path": "dangerzone/6b99acfa5961591c39b3f889cf29970c1dd48ddb0e274f14317940cf279a4412",
    "sha256": "6b99acfa5961591c39b3f889cf29970c1dd48ddb0e274f14317940cf279a4412",
    "yara_possible_family": "asyncrat",
    "key": "eebdb6b2b00c2501b7b246442a354c5c3d743346e4cc88896ce68485dd6bbb8f",
    "salt": "bfeb1e56fbcd973bb219022430a57843003d5644d21e62b9d4f180e7e6c33941",
    "config": {
      "Ports": [
        "2400"
      ],
      "Hosts": [
        "minecraftdayzserver.ddns.net"
      ],
      "Version": "0.5.8",
      "Install": "true",
      "InstallFolder": "%AppData%",
      "InstallFile": "WinRar.exe",
      "Key": "VUpkMU9UTEhRSEVSN2d2eWpLeDJud2Q0STFIcDRXS0U=",
      "Mutex": "LMAsmxp3mz2D",
      "Certificate": "MIIE4DCCAsigAwIBAgIQAM+WaL4OeJIj4I0Usukl1TANBgkqhkiG9w0BAQ0FADARMQ8wDQYDVQQDDA
      "Serversignature": "PBjqcvsYypDmnjgUVv1SkvtLx+jFt2V7NyZ+nHik0CWcLbwOwBXD6/3an89d/I7pFAxwZXgSiL
      "Anti": "false",
      "Pastebin": "null",
      "BDOS": "false",
      "Hwid": "null",
      "Delay": "3",
      "Group": "Default"
    }
  },
  {
    "file_path": "dangerzone/83892117f96867db66c1e6676822a4c0d6691cde60449ee47457f4cc31410fce",
    "sha256": "83892117f96867db66c1e6676822a4c0d6691cde60449ee47457f4cc31410fce",
    "yara_possible_family": "quasarrat",
    "key": "ff230bfb57fecad4bd59d4d97f6883b4",
    "salt": "bfeb1e56fbcd973bb219022430a57843003d5644d21e62b9d4f180e7e6c33941",
    "config": {
      "[illegible]": "1.3.0.0",
```

```
    "[illegible]": "qztadmin.duckdns.org:9782;",
    "[illegible]": 3000,
    "[illegible]": "1WvgEMPjdwfqIMeM9MclyQ==",
    "[illegible]": "NcFtjbDOcsw7Evd3coMC0y4koy/SRZGydhNmno81ZOWOvdfg7sv0Cj5
    "[illegible]": "APPLICATIONDATA",
    "[illegible]": "SubDir",
    "[illegible]": "Client.exe",
    "[illegible]": false,
    "[illegible]": false,
    "[illegible]": "QSR_MUTEX_YMblzlA3rm38L7nnxQ",
    "[illegible]": "Quasar Client Startup",
    "[illegible]": false,
    "[illegible]": true,
    "[illegible]": "mDf8ODHd9XwqMsIxpY8F",
    "[illegible]": "Office04",
    "[illegible]": "Logs",
    "[illegible]": true,
    "[illegible]": false
  }
},
{
  "file_path": "dangerzone/9bfed30be017e62e482a8792fb643a0ca4fa22167e4b239cde37b70db241f2c4",
  "sha256": "9bfed30be017e62e482a8792fb643a0ca4fa22167e4b239cde37b70db241f2c4",
  "yara_possible_family": "venomrat",
  "key": "86cfd98ca989924e7a9439902dc6a72e315da09c11b100c39cd59b9c9372b192",
  "salt": "56656e6f6d524154427956656e6f6d",
  "config": {
    "Ports": [
      "4449"
    ],
    "Hosts": [
      "127.0.0.1"
    ],
    "Version": "Venom RAT + HVNC + Stealer + Grabber  v6.0.3",
    "In_stall": "false",
    "Install_Folder": "%AppData%",
    "Install_File": "speedy",
    "Key": "TzY1S0thald3UGNURmJTYjNSQVdBYlBQR2tTdUFaTTg=",
    "Mutex": "ypxcfziuep",
    "Certifi_cate": "MIICNjCCAZ+gAwIBAgIVALWZXeRliC16frxuoSrGsVJO4U2tMA0GCSqGSIb3DQEBDQUAMGcxFTATB
    "Server_signa_ture": "Sn1WeJuN+Ypb6kUw4QirT1RzbwUEoeSYTmJAIlg0LayMd/VSwAo+0LnnT/g5HFx4QrqaM689
    "Paste_bin": "null",
    "BS_OD": "false",
    "Hw_id": "null",
    "De_lay": "1",
    "Group": "Default",
    "Anti_Process": "false",
```

```
      "An_ti": "true"
    }
  },
  {
    "file_path": "dangerzone/a2817702fecb280069f0723cd2d0bfdca63763b9cdc833941c4f33bbe383d93e",
    "sha256": "a2817702fecb280069f0723cd2d0bfdca63763b9cdc833941c4f33bbe383d93e",
    "yara_possible_family": "quasarrat",
    "key": "None",
    "salt": "None",
    "config": {
      "Version": "1.0.00.r3",
      "RECONNECTDELAY": 5000,
      "PASSWORD": "5EPmsqV4iTCGjx9aY3yYpBWD0IgEJpHNEP75pks",
      "SPECIALFOLDER": "APPLICATIONDATA",
      "SUBFOLDER": "SUB",
      "INSTALLNAME": "INSTALL",
      "INSTALL": false,
      "STARTUP": true,
      "Mutex": "e4d6a6ec-320d-48ee-b6b2-fa24f03760d4",
      "STARTUPKEY": "STARTUP",
      "HIDEFILE": true,
      "ENABLELOGGER": true,
      "Key": "O2CCRlKB5V3AWlrHVKWMrr1GvKqVxXWdcx0l0s6L8fB2mavMqr",
      "Group": "RELEASE",
      "hardcoded_hosts": [
        "kilofrngcida.xyz:443",
        "sartelloil.lat:443",
        "fostlivedol.xyz:443",
        "comerciodepeixekino.org:443",
        "cartlinkfoltrem.xyz:443",
        "trucks-transport.xyz:443"
      ]
    }
  },
  {
    "file_path": "dangerzone/a76af3d67a95a22efd83d016c9142b7ac9974068625516de23e77a5ac3dd051b",
    "sha256": "a76af3d67a95a22efd83d016c9142b7ac9974068625516de23e77a5ac3dd051b",
    "yara_possible_family": "quasarrat",
    "key": "b30cea630f7fac6c2e066ce7f29e1b4bab548ee95b20ff6aa7387ce14df5dc30",
    "salt": "bfeb1e56fbcd973bb219022430a57843003d5644d21e62b9d4f180e7e6c33941",
    "config": {
      "寘褂預ᛒ鉛Ł锐堁翀燱猝畏\"妥鈖": "1.4.1",
      "晜ᙏ袹裸栊渜鱗缝糖귕镀ķ衹摄齪畚": "10.0.0.61:4782;24.67.68.3:4782;",
      "꧀僭ퟏ脖㉿惆舲띊蛐鰲椹撐┘": 3000,
      "轐黵攀轣ᙏ彙觅뱛ㄣ昬灊蕱鎥茨韄븱뻵ᖳ:": "APPLICATIONDATA",
      "빅岑螂철礝庠縴猏脅气縵蜘脖렝": "SubDir",
      "ᯤ ᚏ穱Ƀ巖聂셣쓕簝얣첷蚯觻鄴": "GloomTool.exe",
```

```
    "'🟥씔鉀ᄈ덾稠緘ひ榔枾◌ᵴ□ᄀ ᄭ卫□뻣樑悕": true,
    "컸🟥□愛欹口쏘푂샊'Ꮲ·芯▬젫珚丁 虃㉷虢": true,
    "뻶ᖶ⁄₊ㅠ□筱凶울□巖›□ᘏ ⒷⒷ娩抢落": "9fdd3e80-d560-431b-b526-3ebbc1799110",
    "鰷🟥眩ㅃ잴"Ḥ넕蛟须ᄒ Ⓐ摯킋扼뿇≤Ⱡ□랔考": "WindowsAV",
    "떐吳盃⁞哼⁞□♉瞸긿⃠ 🟥崾�ꗃ ̛淯枴崇킔": true,
    "汄쩽检퓔鴒远⣿둻□中頑„筎ᵕㅁ軮瘭렗蹜濱": true,
    "㎛佟칐ㄷ韶ᶣ놷崘娖媲ㅓ躅픎□ᵢ₎ ᄒ🟥殧□□": "5F91B88C67A9ACF78B2396771B3B6F2B4615CA57",
    "숸윓ₚF滬ⓝ.𝌆頧□排溳昀讓툚顓훲□□": "Office04",
    "맖ᨕƁ嫈悼�꾛둅薙鸚–�坦챹□탏琅峒□乂": "Logs",
    "⣿嶱맊嘯패熟墊□砫□뱧 ｉ ◆□ㄱ菜□": "KQrwmpZSwOF20ZdNZlVJ7YjgErzUf9cophPOCAULRI4gSid7qeSaRL4LhhUX
    "🟥醓酸惦싰註楹揽첆稦설嶺肭ᆠ뀷甒홤囤": "MIIE9DCCAtygAwIBAgIQAIhqXB+nLwd+VvEk3rjLsTANBgkqhkiG9
    "撂嗌渌냧✷엳!◆□暐쀳쁾瘣굇ᵽ๑珮饆猢": true,
    "🅉Ḛ錌≠琰锜艑닅□썳宓幂즆閞◆㉦轎□跂楞": true,
    "뇯뾘◆厥Ծ甙鵟獩짐˝助멁ḱ拐豷┭皿롞愚樟": "",
    "□鯠讀◆◆c鏾鬣◆行彳圾딧頷□꾕內竚●": "",
    "剔壴嗇켜ᵥ□穴靂懍嶰顱硝芹慹麋□满境🟥□": true
  }
},
{
  "file_path": "dangerzone/b5bff486f091f9539606931e0aff280eaea17064b2a12940675dfac926e9666e.exe",
  "sha256": "b5bff486f091f9539606931e0aff280eaea17064b2a12940675dfac926e9666e",
  "yara_possible_family": "xworm",
  "key": "c527ac2a4eeb6039d9477583d0f4f2c527ac2a4eeb6039d9477583d0f4f2ee00",
  "salt": "None",
  "config": {
    "Hosts": [
      "act-cleaning.gl.at.ply.gg"
    ],
    "Ports": [
      "37158"
    ],
    "KEY": "<123456789>",
    "SPL": "<Xwormmm>",
    "Sleep": 3,
    "Group": "NeverLoseCrack",
    "USBNM": "USB.exe",
    "InstallDir": "%ProgramData%",
    "InstallStr": "svchost.exe",
    "Mutex": "OkWVOTioL6k3Fg3w",
    "LoggerPath": "\\Log.tmp"
  }
},
{
  "file_path": "dangerzone/beb1b5cd2a33e86e48599b183b882fc3e80198a8062e5b9d9251e605d3f0bfd5.exe",
  "sha256": "beb1b5cd2a33e86e48599b183b882fc3e80198a8062e5b9d9251e605d3f0bfd5",
  "yara_possible_family": "quasarrat",
  "key": "b5580a84ddadcf548713dd64fedbbe067f931e6ce4699271de572acbd52f4074",
```

```
    "salt": "bfeb1e56fbcd973bb219022430a57843003d5644d21e62b9d4f180e7e6c33941",
    "config": {
      "伉雂婀瀫ざ□□昄뙖셟뾲▯헦榱僝콪絜鍮緒쪖": "1.4.1",
      "�낧胃櫐臽塽뾞珅⬆郜□□ゐ곷閞創玊□騆镲": "91.92.241.122:6969;",
      "騷⛴□□ㅓ獐笁□앮閞컨ᵎ綟麩墐◌屻烅□": 3000,
      "숀덢衕ᄀ ᩚ鬮ж욤쬁誁佁□푈⛐⊙闢□퍽닢": "APPLICATIONDATA",
      "ᩚ 툞⤑퓩僗膜弊溳 ᡈ렦□圢◆□⍟□騺蟗Sv좟": "",
      "'ꂹ 쬀믍□□□ 贕好顆賞柊ㅓ 钵∧멃B螑餚": "Client.exe",
      " ∞白魶咒□□ᵡ瘢笵ᵕ畎錡읐ᚼ簞웤侏骸□옍": true,
      "斐□□苛뾆傗ʁ呈헉遁骗ᇂ 珍㶏洇鱷뾆藆꽻祗": true,
      "簑쌑饒曰姞輪MV鑸鯉ᵴ 掾ᡣ싻□□□캥伽": "fcf2be0a-a426-40c6-b153-1a354814f80d",
      "磛瑸鮣籾쬗ᦉ帝蝬騿鐪긂□듗ᥒ엮□螑□": "Quasar Client Startup",
      "鵁x鬳詗ᶻ㊥据□日ᵷ ll 荧ᡱ夾ʰᚳ 뾱□鎘뜯": false,
      "壖輁絫□鱎鰍崛娡揑웳葍視篢豆ᡡ竭蟋뾽菈鍵": true,
      "嘛⣿□鏢伊□暈者梓匆銳I秩戮鬫□獵櫟ᩚ蠔": "26A6C07FE7354BCD244B108D2E3538DCF04477F5",
      "凹콫屜□鱎 ᦓ㨦烳箄騃쉳훚扑□礗澶滶뵠逃": "Fab",
      "ᠰ빉뢮뢜刃ᄆ垉迄湎鯙ᩫ稽 ᄇ瘜□é⋆厎嗎": "Logs",
      "-ᅠ宋疝亞꿛牀□漩덯蟭빉悠뼞櫻빜⑴◉ ᄋ ᖶ_ᆡ": "U/jVlmjpH/9zMrLFla8LcLavxUQe9wt9L6qGAh9zYqPdqDW0e0f
      "霧獙□ᄋ◉稜❽柿曉즛□쿾坯뗋툪ᦒ□": "MIIE9DCCAtygAwIBAgIQAJMC1KOnf3PAJ47sO2MclTANBgkqhkiG9w0BAQ0F
      "□嵥帳迟읍ㅂ遞|一ᡬ 짒ㅂ샖쮟铒ᄼᡱ愾콕萊": false,
      "◌ㅠ巨騆般髮鷞毡粖鉦□宸켡-ᅠ□⚾龔□薮": false,
      "ᓚᑭ膹蔭騷労酮ᑐᐟ篶ш蚼좓●脬랖□팩癱": "",
      "□亡늣漊ᘐ ᢐ몤뒤짚핿ʁ ᯅ 昇뉂搥囡롷巒Ð": "",
      "ᄑ㉤绒꼿◉患酁皜喫翔ᵏᄀ ᵍ氖ᑫ젦霆ᐊᐬ醅": true
    }
  },
  {
    "file_path": "dangerzone/d5028e10a756f2df677f32ebde105d7de8df37e253c431837c8f810260f4428e",
    "sha256": "d5028e10a756f2df677f32ebde105d7de8df37e253c431837c8f810260f4428e",
    "yara_possible_family": "xenorat",
    "key": "650f47cdd14eaef8c529f2a03fa7744c",
    "salt": "None",
    "config": {
      "Hosts": [
        "77.221.152.198"
      ],
      "Ports": 4444,
      "Key": "03ac674216f3e15c761ee1a5e255f067953623c8b388b4459e13f978d7c846f4",
      "delay": 5000,
      "mutex_string": "Xeno_rat_nd89dsedwqdswdqwdwqdqwdqwdwqdwqdqwdqwdwqdwqd12d",
      "DoStartup": 2222,
      "Install_path": "appdata",
      "startup_name": "nothingset"
    }
  },
  {
    "file_path": "dangerzone/db09db5bdf1dcf6e607936a6abbe5ce91efbbf9ce136efc3bdb45222710792fa",
```

```
    "sha256": "db09db5bdf1dcf6e607936a6abbe5ce91efbbf9ce136efc3bdb45222710792fa",
    "yara_possible_family": "venomrat",
    "key": "11ed70df5ce22de750c6e7496fa5c51985c321d2d9dd463979337af003644f41",
    "salt": "56656e6f6d524154427956656e6f6d",
    "config": {
      "Ports": [
        "4449",
        "7772"
      ],
      "Hosts": [
        "127.0.0.1"
      ],
      "Version": "Venom RAT + HVNC + Stealer + Grabber  v6.0.3",
      "In_stall": "false",
      "Install_Folder": "%AppData%",
      "Install_File": "",
      "Key": "M1NoWkREazBvNTNGUkRlT0s4TjE1QlRRQmx4bW1zd2U=",
      "Mutex": "qmhvogiycvwh",
      "Certifi_cate": "MIICOTCCAaKgAwIBAgIVAPyfwFFMs6hxoSr1U5gHJmBruaj1MA0GCSqGSIb3DQEBDQUAMGoxGDAWB
      "Server_signa_ture": "BW9mNNWdLZ+UgmfSTOot753DE24GfE+H6HYG5yl4IFszdMLpfQXijxVlt3bcz68PrHwYG2R7
      "Paste_bin": "null",
      "BS_OD": "false",
      "Hw_id": "null",
      "De_lay": "1",
      "Group": "Default",
      "Anti_Process": "false",
      "An_ti": "false"
    }
  },
  {
    "file_path": "dangerzone/fb0d45b0e48b0cdda2dd8c5a152f3c7a375c18d63e588f6a217c9d47f7d5199d",
    "sha256": "fb0d45b0e48b0cdda2dd8c5a152f3c7a375c18d63e588f6a217c9d47f7d5199d",
    "yara_possible_family": "xworm",
    "key": "e5f7efe2fddd6755c92cbc39d5559ce5f7efe2fddd6755c92cbc39d5559c4000",
    "salt": "None",
    "config": {
      "aumDBZNDJ7f2": "mo1010.duckdns.org",
      "gnnrkMjhrGnD": "7000",
      "xeGVxN2u4Sp3": "<123456789>",
      "upgseICLHsZe": "<Xwormmm>",
      "jF5pyMR4K1B8": 3,
      "VpYiyt9aVUsv": "USB.exe",
      "z7mwUS4LmaFC": "%AppData%",
      "Fjg9TdM4RTsH": "tBZ7NDtphvUCm0Dc",
      "5BPKEMIKpcCV": "\\Log.tmp"
    }
  },
```

```
{
  "file_path": "dangerzone/vstdlib_s64",
  "sha256": "6e5671dec52db7f64557ba8ef70caf53cf0c782795236b03655623640f9e6a83",
  "yara_possible_family": "quasarrat",
  "key": "526f35346a62726168486530765a6266487a703968557552663768 4a737575794b4c7933654e5a3465644c41
  "salt": "None",
  "config": {
    "Version": "1.0.00.r6",
    "RECONNECTDELAY": 5000,
    "PASSWORD": "5EPmsqV4iTCGjx9aY3yYpBWD0IgEJpHNEP75pks",
    "SPECIALFOLDER": "APPLICATIONDATA",
    "SUBFOLDER": "SUB",
    "INSTALLNAME": "INSTALL",
    "INSTALL": false,
    "STARTUP": true,
    "Mutex": "e4d6a6ec-320d-48ee-b6b2-fa24f03760d4",
    "STARTUPKEY": "STARTUP",
    "HIDEFILE": true,
    "ENABLELOGGER": true,
    "Key": "O2CCRlKB5V3AWlrHVKWMrr1GvKqVxXWdcx0l0s6L8fB2mavMqr",
    "Group": "RELEASE",
    "xor_decoded_strings": [
      "BPN - Nuestro Banco",
      "Red Link - bpn",
      "HB Judiciales BPN",
      "Ingresá a tu cuenta",
      "Online Banking Web",
      "Banca Empresa 3.0",
      "Banco Ciudad",
      "Banco Ciudad | Autogestión",
      "Banca Empresa 3.0",
      "Banco Comafi - Online Banking",
      "Banco Comafi - eBanking Empresas",
      "Online Banking Santander | Inicio de Sesión",
      "Online Banking Empresas",
      "Online Banking",
      "Office Banking",
      "HSBC Argentina",
      "HSBC Argentina | Bienvenido",
      "accessbanking.com.ar/RetailHomeBankingWeb/init.do?a=b",
      "ICBC Access Banking | Home Banking",
      "Banco Patagonia",
      "ebankpersonas.bancopatagonia.com.ar/eBanking/usuarios/login.htm",
      "Página del Banco de la Provincia de Buenos Aires",
      "Red Link",
      "bind - finanzas felices :)",
      "BindID Ingreso",
```

```
        "BBVA Net Cash | Empresas | BBVA Argentina",
        "Bienvenido a nuestra Banca Online | BBVA Argentina",
        "Ingresá tu e-mail, teléfono o usuario de Mercado Pago",
        "Mercado Pago | De ahora en adelante, hacés más con tu dinero.",
        "Mercado Pago",
        "Home Banking",
        "Office Banking",
        "Banco Santa Cruz Gobierno - Una propuesta para cada Comuna o Municipio | Banco Santa Cruz",
        "Home banking",
        "Office Banking",
        "Banco de Santa Cruz",
        "Red Link",
        "Banco de la Nación Argentina",
        "Red Link - BANCO DE LA NACION ARGENTINA",
        "Red Link",
        "Macro | Agenda powered by Whyline",
        "Banco Macro | Banca Internet Personas",
        "Banco Macro | NUEVA Banca Internet Empresas",
        "https://argentina-e4162-default-rtdb.firebaseio.com/user.json",
        "C:\\\\Users\\\\",
        "\\\\AppData\\\\Local\\\\Aplicativo Itau",
        "C:\\\\Program Files\\\\Topaz OFD\\\\Warsaw",
        "C:\\\\ProgramData\\\\scpbrad",
        "C:\\\\ProgramData\\\\Trusteer",
        "dd.MM.yyyy HH:mm:ss",
        "application/json",
        "Sistema no disponible, intente nuevamente más tarde.",
        "SENHA DE 6 BPN",
        "SENHA DE 6 NB",
        "SENHA DE 6 CIUDAD",
        "SENHA DE 6 COMAFI",
        "SENHA DE 6 GALACIA",
        "SENHA DE 6 HSBC",
        "SENHA DE 6 ICBC",
        "SENHA DE 6 PATAGONIA",
        "SENHA DE 6 PROVINCIA",
        "SENHA DE 6 SANTANDER",
        "SENHA DE 6 BIND",
        "SENHA DE 6 BBVA",
        "driftcar.giize.com:443",
        "adreniz.kozow.com:443"
      ]
    }
  }
]
```

Development Guide

More Verbose Guide To Be Published

Development Dependencies

RKP uses `pre-commit` to enforce formatting.

To begin development and install `pre-commit`, use the following command:

Then, ensure you install the pre-commit hook:

Feedback, Issues, and Additions

If you have suggestions for improvement, bugs, feedback, or additional RAT families that use a similar configuration format as AsyncRAT, QuasarRAT, VenomRAT, DcRAT, etc. that are not yet supported, please send me a message on Bluesky, YouTube, or submit an Issue or PR in this repo.

Also, if this tool or video tutorial was helpful to you, that's always nice to hear as well!

Thank you!

Contributions & Attribution

Huge thanks to the following contributors for their outstanding work:

- doomedraven: For your help in integrating RKP into CAPEv2, as well as your continued contributions to the project as a coauthor
- cccs-rs: For your help in integrating RKP into AssemblyLine, as well as helping me wrap it to work with MACO

The logo for this project contains modifications of the following images:

- Ouroboros (modified) - Image by Freepik - https://www.freepik.com/free-vector/ouroboros-symbol-illustration_37368320.htm
- Rat King Illustration (modified) - User:Di (they-them), CC BY 4.0 https://creativecommons.org/licenses/by/4.0, via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:Rat_King_Illustration.svg

---