

FrenchCisco/RATel

 github.com/FrenchCisco/RATel

FrenchCisco



RATel

Language [Python3](#) Language [C++](#) Language [SQL](#) Version [Beta](#) License [MIT](#) commit activity [0/month](#)
[Stars](#) [224](#) [Visitor](#) [24224](#)



Please do not upload to virustotal !



To prevent RATel from being detected by antivirus, please do not upload the payload to TOTAL VIRUS.

Each month I will test myself if the payload gets detected by antivirus.

So you'll have a photo every month to prove RATel discretion.

Description

RAT-el is an open source penetration test tool that allows you to take control of a windows machine.

It works on the client-server model, the server sends commands and the client executes the commands and sends the result back to the server.

The client is completely undetectable by anti-virus software.

Screenshots

```
Z:\server>py RATelServer.py --port 4444 --clean
RAT-el Server BETA
[?] By default, the connection display is active.To avoid being generated, you can deactivate it with the -cdd command.
[?] Run -h or --help to list the available commands.
RATelServer>
```

```
RATelServer> --list
[?] Command execute: ['--list']
```

Session	IP	Port	Is he alive	Is he admin	Path RAT	Username
0	127.0.0.1	50067	True	cisco	Z:\payload\rat1.exe	cisco
1	127.0.0.1	50068	True	cisco	Z:\payload\rat2.exe	cisco
2	127.0.0.1	50069	True	cisco	Z:\payload\rat3.exe	cisco
3	127.0.0.1	50070	True	cisco	Z:\payload\rat1.exe	cisco
4	127.0.0.1	50071	True	cisco	C:\Users\cisco\Desktop\rat3.exe	cisco
5	127.0.0.1	50072	True	cisco	C:\Users\cisco\Documents\rat3.exe	cisco
6	127.0.0.1	50073	True	cisco	C:\Users\cisco\Pictures\rat3.exe	cisco
7	127.0.0.1	50074	True	cisco	C:\Users\cisco\Pictures\Camera Roll\rat3.exe	cisco
8	127.0.0.1	50075	True	cisco	C:\Users\cisco\Pictures\Camera Roll\rat3.exe	cisco
9	127.0.0.1	50076	True	cisco	C:\Users\cisco\Pictures\Camera Roll\rat3.exe	cisco
10	127.0.0.1	50077	True	cisco	C:\Users\cisco\Pictures\Camera Roll\rat3.exe	cisco
11	127.0.0.1	50078	True	cisco	C:\Users\cisco\Documents\rat3.exe	cisco
12	127.0.0.1	50079	True	cisco	C:\Users\cisco\Documents\rat3.exe	cisco
13	127.0.0.1	50080	True	cisco	C:\Users\cisco\Documents\rat3.exe	cisco
14	127.0.0.1	50081	True	cisco	C:\Users\cisco\Documents\rat3.exe	cisco
15	127.0.0.1	50082	True	cisco	C:\Users\cisco\Documents\rat3.exe	cisco

```
RATelServer>
```

2 / 170

Community Score

2 engines detected this file

6df70f080a4f8225fdd1fecdd58554f6ba8ff22adc3225ae7df0638d8cf4eec

FrenchCisco.exe

986.50 KB Size | 2021-02-20 10:44:32 UTC a moment ago

EXE

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
SecureAge APEX		Malicious	Unsafe
Acronis		Undetected	Undetected
AegisLab		Undetected	Undetected
Alibaba		Undetected	Undetected
Antiy-AVL		Undetected	Undetected
Avast		Undetected	Undetected
Baidu		Undetected	Undetected
BitDefenderTheta		Undetected	Undetected
CAT-QuickHeal		Undetected	Undetected
CMC		Undetected	Undetected
CrowdStrike Falcon		Undetected	Undetected
Cynet		Undetected	Undetected

Added features

Features

RATelServer:

- Multiple Connections
- Broadcast commands to all clients
- Stores client informations in the database
- Encryption of data on the network via XOR
- Token management system to identify clients
- Unicode management

Client:

- Encryption of data send over the network
- Startup persistence
- Remote command execution via CMD
- Remote command execution via Powershell
- Encryption of data on the network via XOR
- Automatic persistence when running the client
- Automatic reconnection
- Unicode management

RATelGenerator:

Automatic client compilation

Documentations

- **Installations:**
- [Windows Installation](#)
- [Linux Installation](#)

- **RATelServer:**
 - [Arguments RATelServer](#)
 - [Usage RATelServer](#)
 - [RATelGenerator](#)
 - [Simple usage](#)
 - **Advanced usage:**
 - [Demonstration video](#)
-

Future features

Keylogger for the version: **beta_v0.2**

Motivation

I decided to create this project to improve my C++ skills, to learn new notions I didn't know and to learn English.

I intend to maintain and improve the project continuously by adding new features.

Informations

If you are interested in the development of my RATel project and would like to contribute to it, please contact me by email (juanrubio.dev@gmail.com).

If you have any ideas for features, code improvements or bugs, you can leave me a issues.

Disclaimer:

The use of this software on any device that is not yours is prohibited. If you use RATel on a machine that does not belong to you, I will in no way be responsible for your actions.
