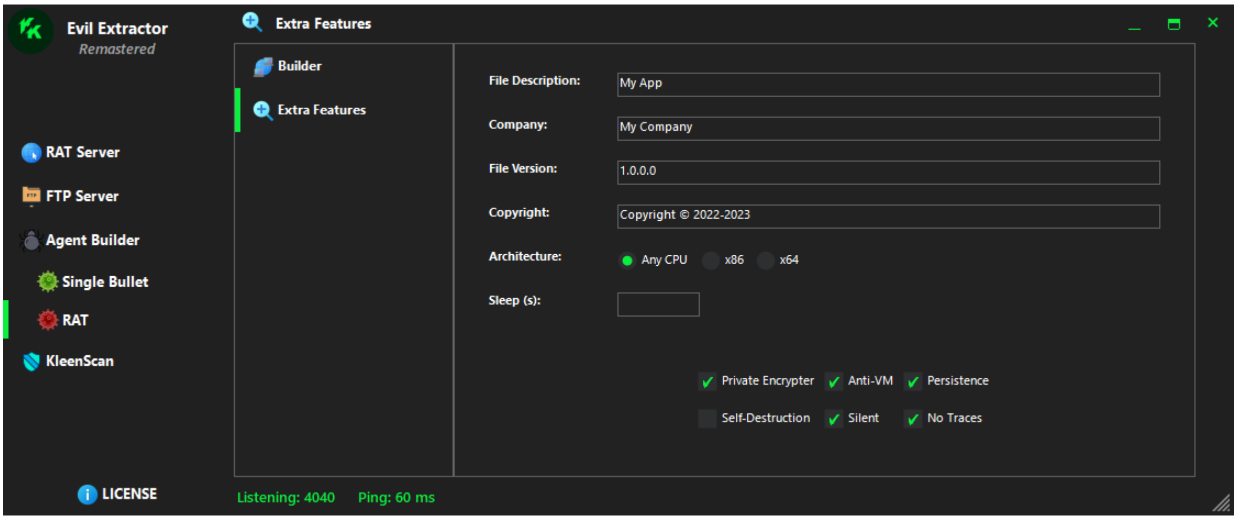
Last Updated: **July 16, 2024**

Overview

(RAT)

1) Extra Features



File Description: My App

Company: My Company

File Version: 1.0.0.0

Copyright: Copyright © 2022-2023

Architecture: ● Any CPU ○ x86 ○ x64

Sleep (s):

☑ Private Encrypter ☑ Anti-VM ☑ Persistence

☐ Self-Destruction ☑ Silent ☑ No Traces

Listening: 4040 Ping: 60 ms

Before creating your RAT Agent, you can take a look at "Extra Features" section. Your agent will be created referencing this section:

Assembly Configuration:

1) File Description (optional)

2) Company Name (optional)

3) File Version (required)

4) Copyright (optional)

5) Architecture (required)

Other Features:

1) Sleep (optional):

This option determines how many seconds your agent should sleep before executing the main code.

2) Private Encrypter (optional):

This option allows you to encrypt your agent and make the source more complicated (using the AES encryption algorithm). This is solely for safeguarding personal information and the structure of the program.

3) Anti-VM (optional):

This option enables Anti-VM, which means your agent will not work on any virtual machine. Also, if any reverse-engineering tool is running, the agent will not function.

4) Persistence (optional):

This option allows you to make your agent persistence on the target system. It cannot used with self-destruction module.

5) Self-Destruction (optional):

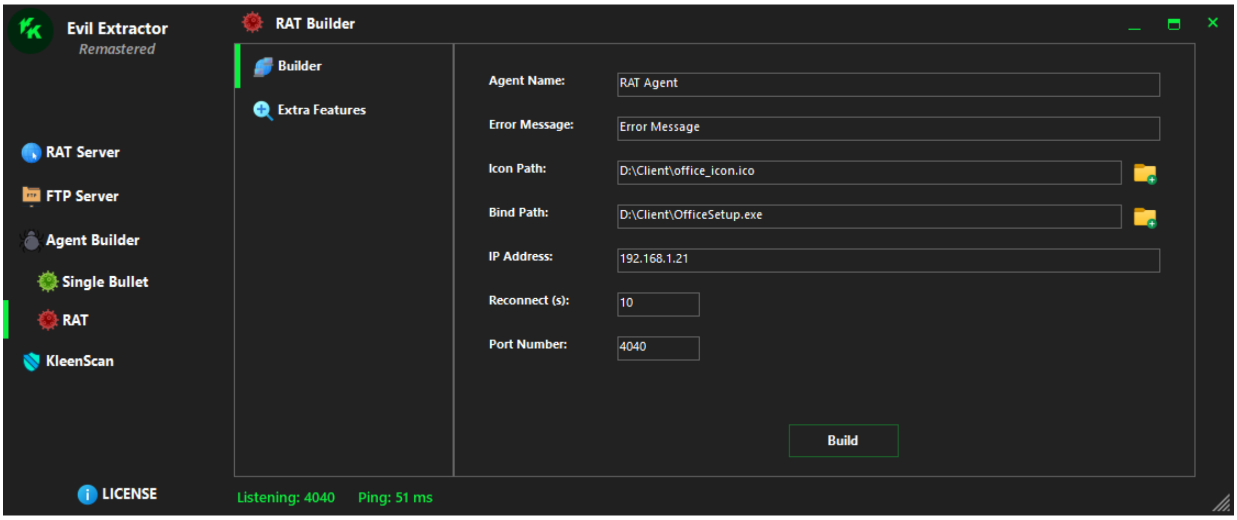
If this option checked, your agent will self-destruct after you decide to kill the session. It cannot used with persistence module.

6) Silent (optional):

This option allows you to make your agent fully silent on the target system.

7) No Traces (optional):
This option ensures that your agent does not leave traces on the target system.

2) Creating your RAT Agent



Agent Name: RAT Agent

Error Message: Error Message

Icon Path: D:\Client\office_icon.ico

Bind Path: D:\Client\OfficeSetup.exe

IP Address: 192.168.1.21

Reconnect (s): 10

Port Number: 4040

After filling out the Extra Features section as you desire, you're ready to create your RAT Agent:

1) Agent Name (required)

2) Error Message (optional)

3) Icon Path (optional)

4) Bind Path (optional):

You can bind your agent with the following file types: exe, pdf or image files (jpg or png).
Note: File size is limited with 100 MB. Binder also integrated with persistence module(s). If you bind any file with one of our persistence module(s), your agent will work successfully but additional file will not open at windows startup.

5) IP Address (mydomain.com or X.X.X.X, it's required):

If you are going to use your RAT agent on the public network, then you have to type your public IP Address in this section. Otherwise, you can type your local IP Address.
Note: This section supports domain names. That means, you can use duckdns or other similar services, if you know how to use it.

6) Reconnect (optional):

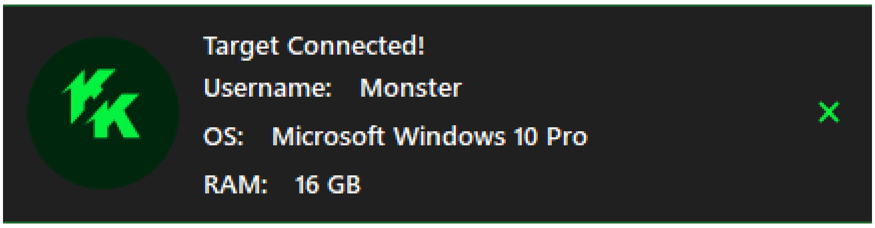
Recommended. This option allows the target system to reconnect to you after x seconds in case of any corruption.

7) Port Number (required)

Default agent size: 806 KB

3) RAT Server

You will receive a notification when your RAT agent is running on the target system:



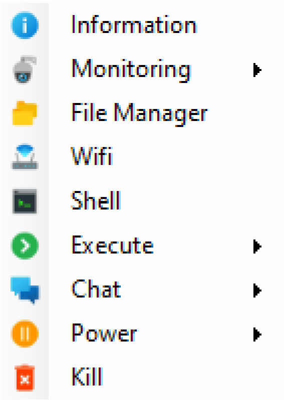
Target Connected!

Username: Monster

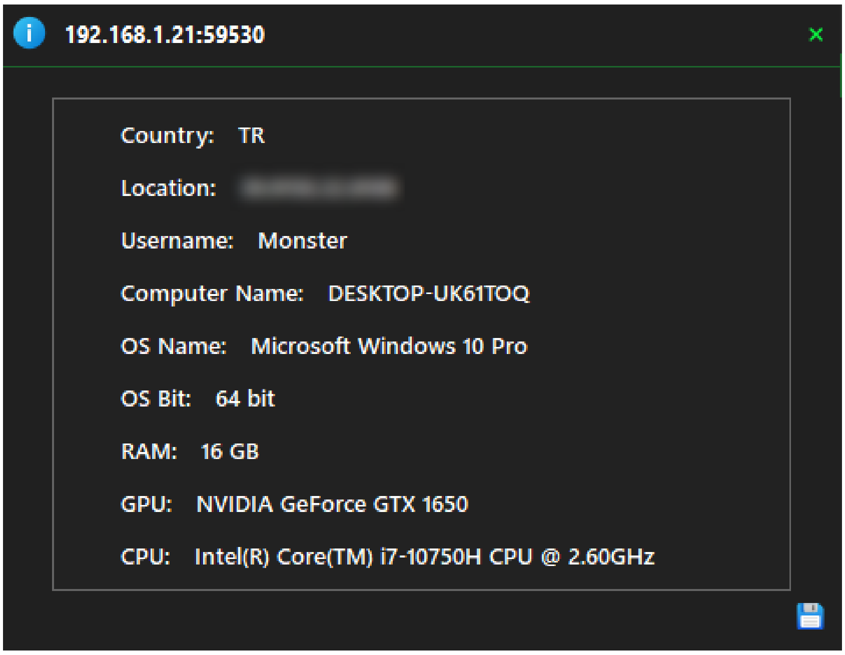
OS: Microsoft Windows 10 Pro

RAM: 16 GB

Now, you are ready to take actions:



1) Information



192.168.1.21:59530

Country: TR

Location: [redacted]

Username: Monster

Computer Name: DESKTOP-UK61TOQ

OS Name: Microsoft Windows 10 Pro

OS Bit: 64 bit

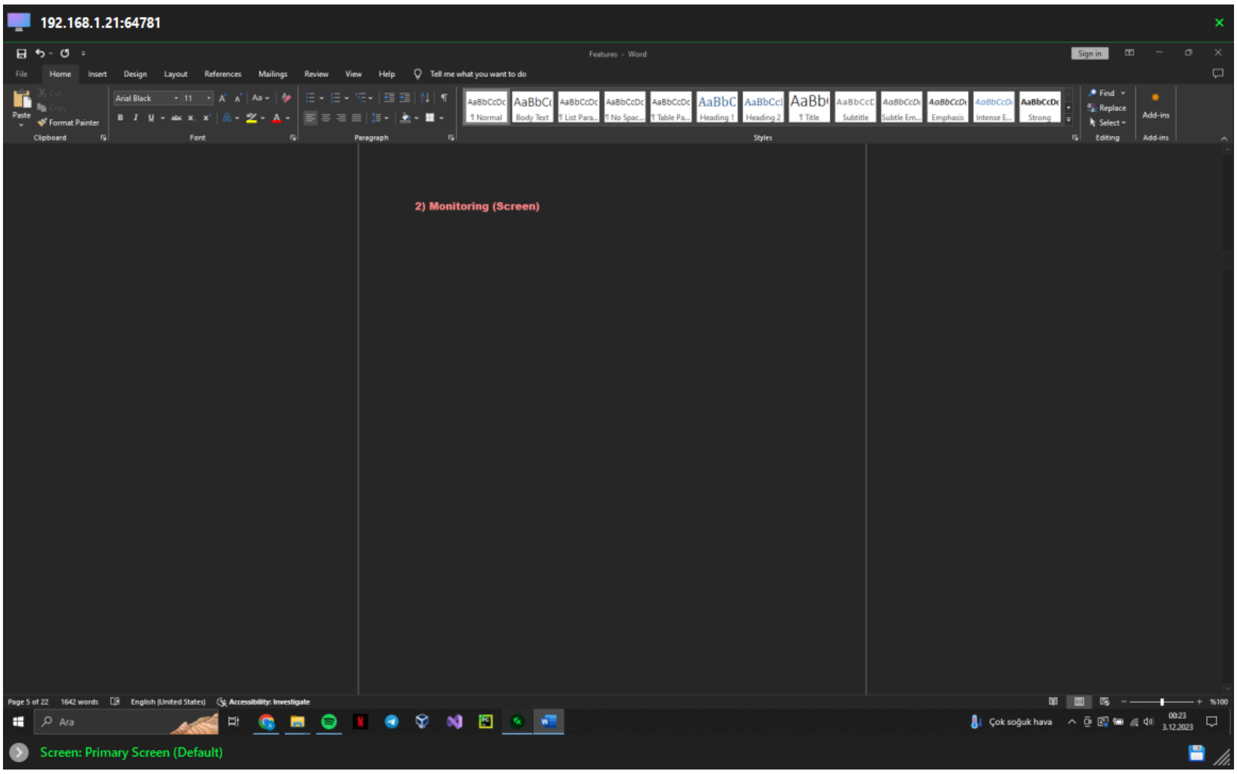
RAM: 16 GB

GPU: NVIDIA GeForce GTX 1650

CPU: Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz

General information about the target system can be accessed through this tab, and if you wish, you can click on the 'Save' icon at the bottom right to save it to your local computer.

2) Monitoring (Screen)

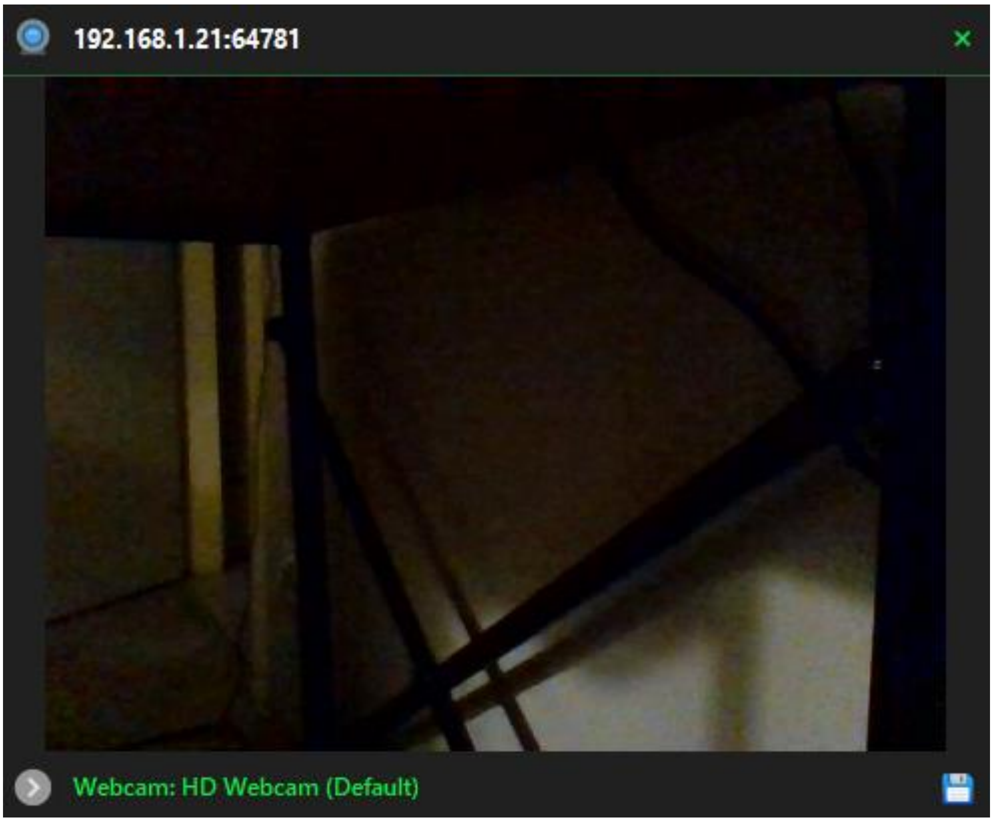


192.168.1.21:64781

Screen: Primary Screen (Default)

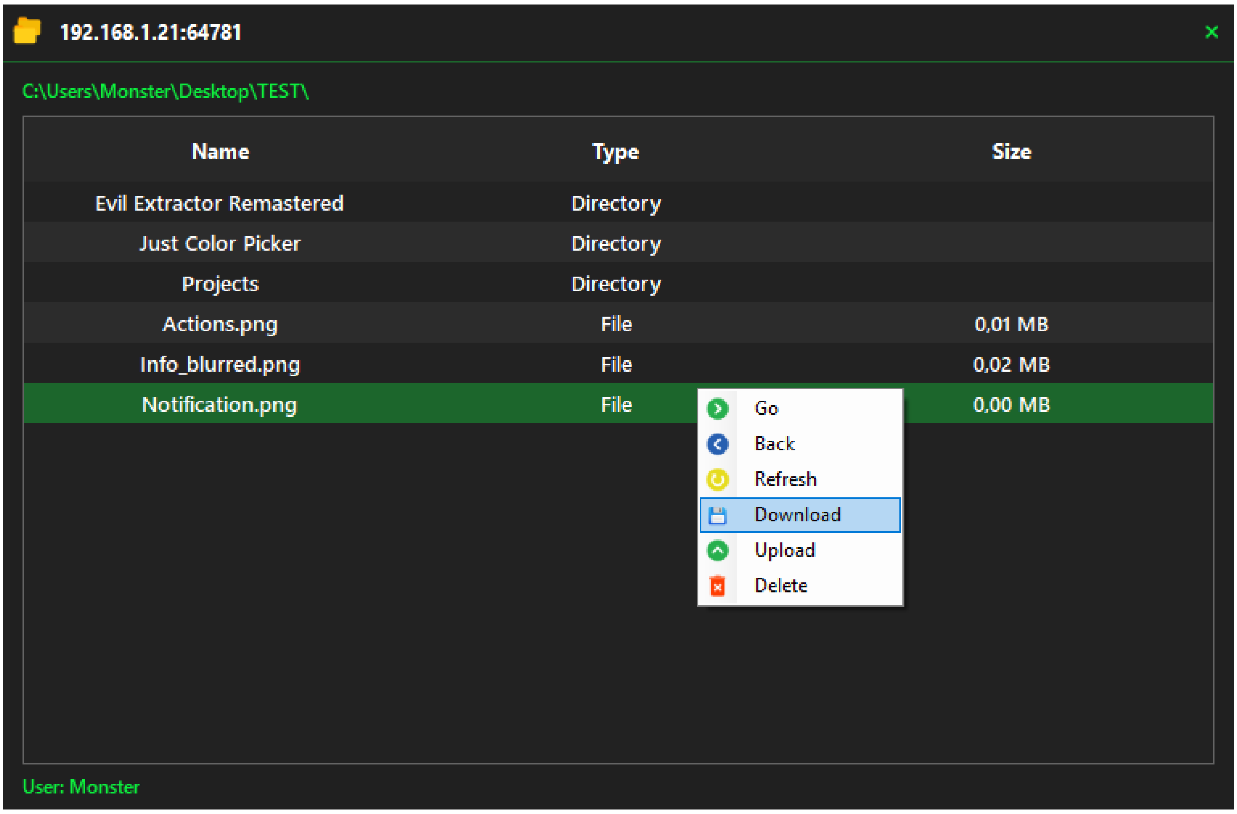
Right now, you can see me while preparing this documentation :) As you can see, this option allows you to live monitor the screen of the target system and take screenshots as desired.

3) Monitoring (Webcam)



As you can see, this option allows you to live monitor the webcam of the target system and take screenshots as desired.

4) File Manager



192.168.1.21:64781

C:\Users\Monster\Desktop\TEST\

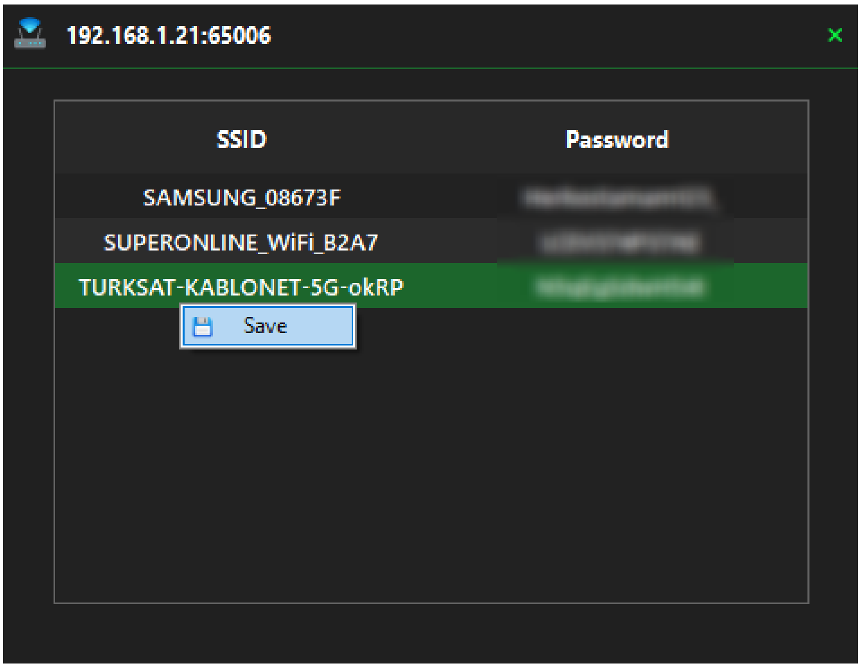
Name	Type	Size
Evil Extractor Remastered	Directory	
Just Color Picker	Directory	
Projects	Directory	
Actions.png	File	0,01 MB
Info_blurred.png	File	0,02 MB
Notification.png	File	0,00 MB

User: Monster

You can think of the File Manager feature as if you've opened an invisible file explorer on the target system. With this option, you can delete, upload (from your local computer), download files (to your local computer), and navigate between folders on the target system.

Note: Allowed file size for download & upload is a maximum of 400 MB.

5) WIFI

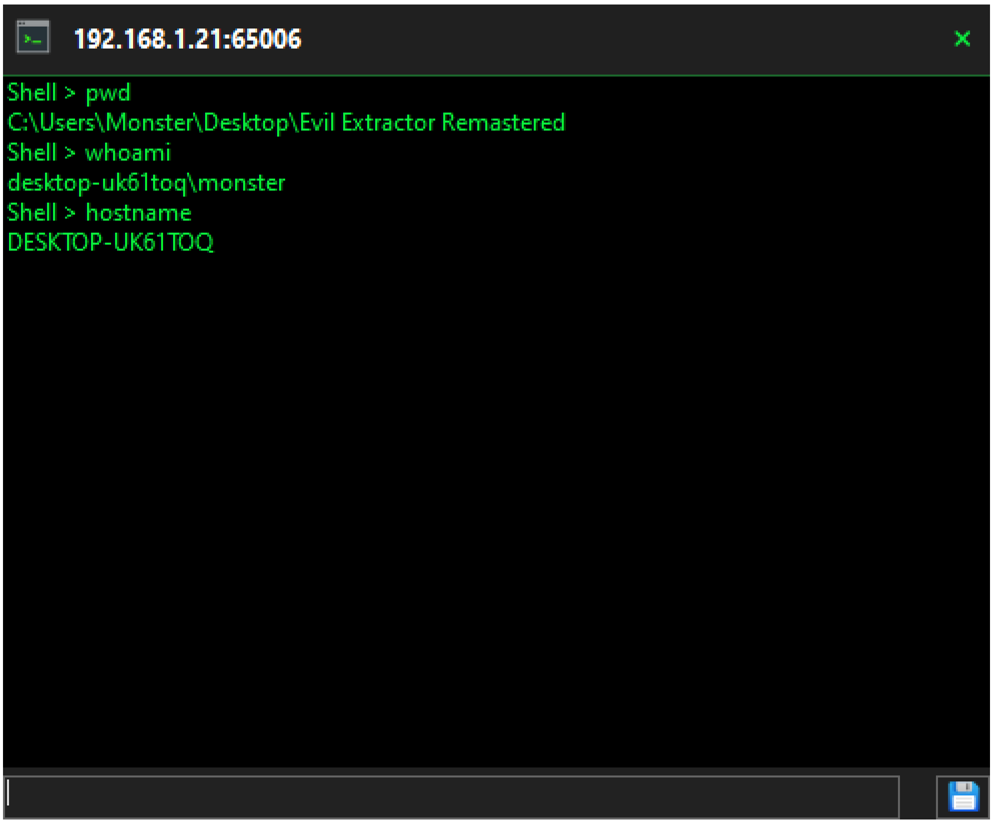


192.168.1.21:65006

SSID	Password
SAMSUNG_08673F	[redacted]
SUPERONLINE_WiFi_B2A7	[redacted]
TURKSAT-KABLONET-5G-okRP	[redacted]

This option retrieves the names and passwords of all WIFI networks on the target system (if there are no registered WIFI networks, this section will appear empty). You can right-click to save all this information to your local computer.

6) Shell (Cmd)



```
Shell > pwd
C:\Users\Monster\Desktop\Evil Extractor Remastered
Shell > whoami
desktop-uk61toq\monster
Shell > hostname
DESKTOP-UK61TOQ
```

In this section, you can execute (available) commands on the target system. Available commands:

Commands

----

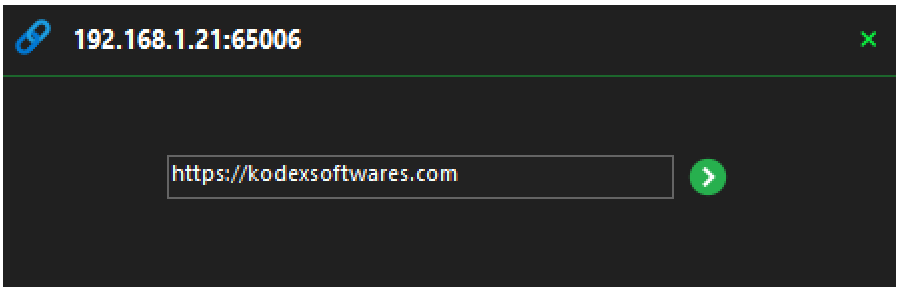
clear/cls	**-> clear the screen**
dir	**-> list files/directory**
pwd	**-> show current directory**
mkdir *name*	**-> make directory**
cat *txt file*	**-> read file content**
whoami/hostname	**-> learn machine id**
mkdir *name*	**-> make directory**
cd *directory name*	**-> changes directory**
del *file name*	**-> delete file or directory**
start *process*	**-> execute process, url or file**
exit	**-> close shell**

Advanced Commands

----

ipconfig	**-> network configuration info**
netsh wlan show profile	**-> show netsh info**

7) Execute (URL)

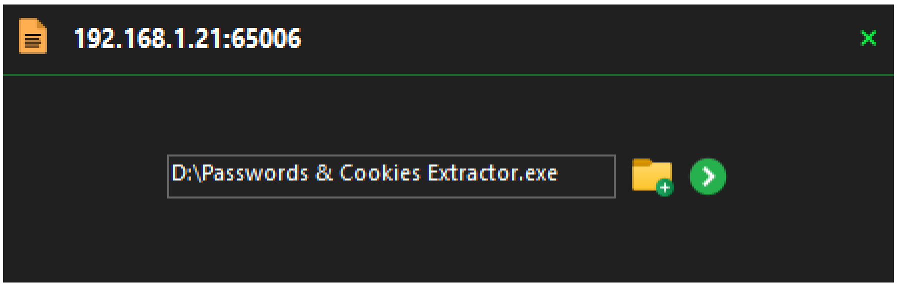


192.168.1.21:65006

https://kodexsoftwares.com

In this section, you'll be able to execute (open) desired URL on the target system's browser.

8) Execute (File)



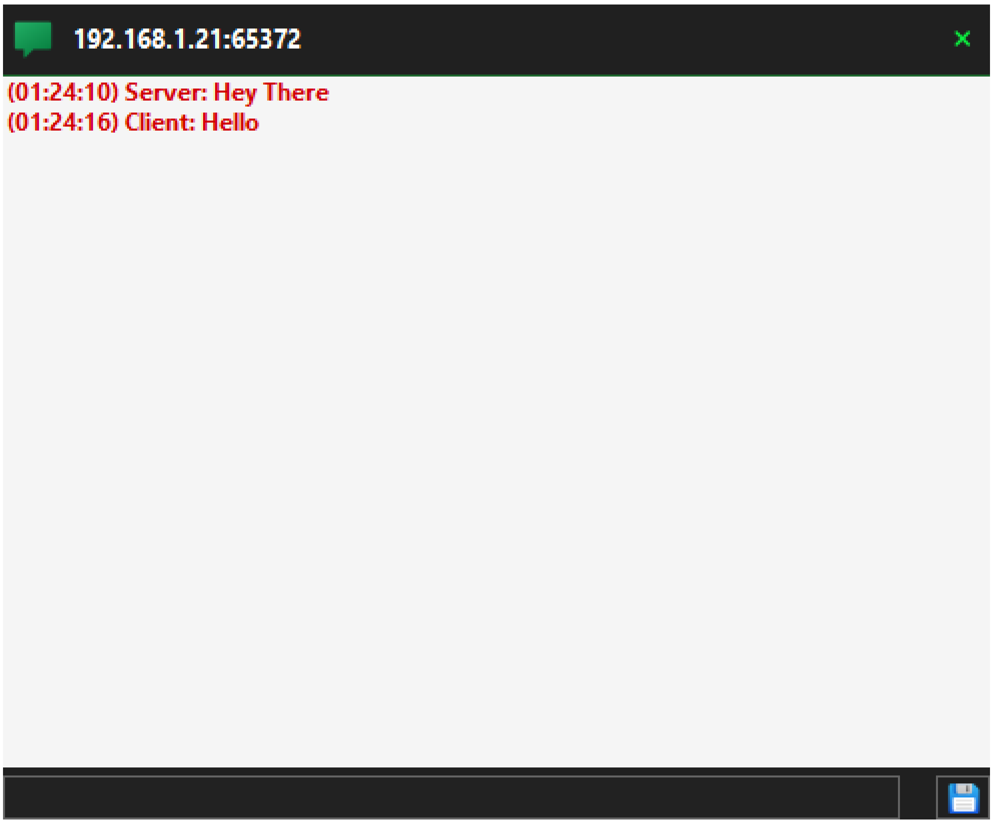
192.168.1.21:65006

D:\Passwords & Cookies Extractor.exe

Execute File option silently uploads an exe, jpg, png or pdf file from your local computer to the target system and then runs the uploaded file instantly.

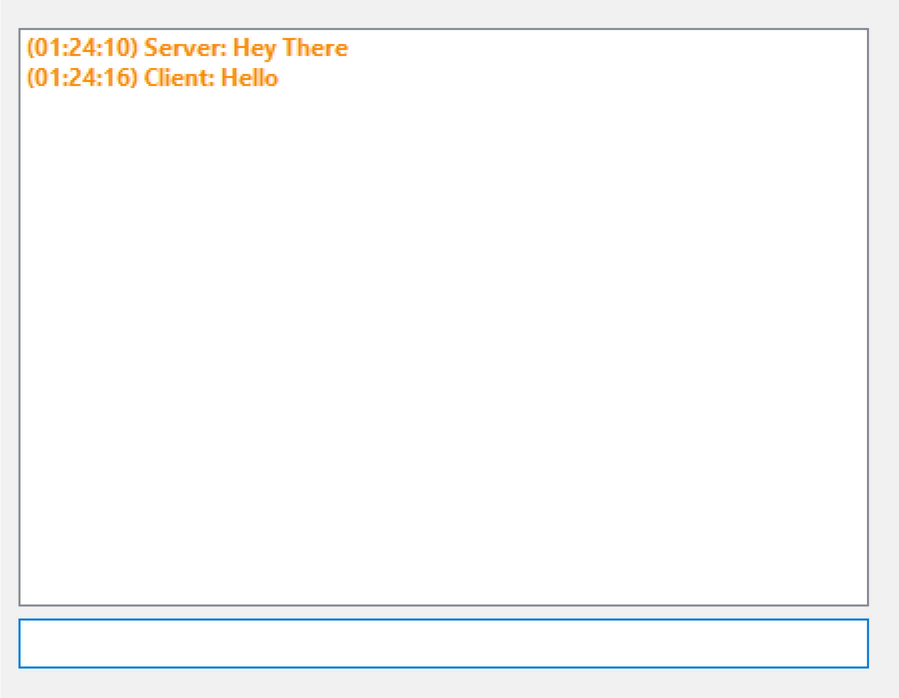
Note: Allowed file size for upload & execute is a maximum of 400 MB.

9) Chat (Live Chat)



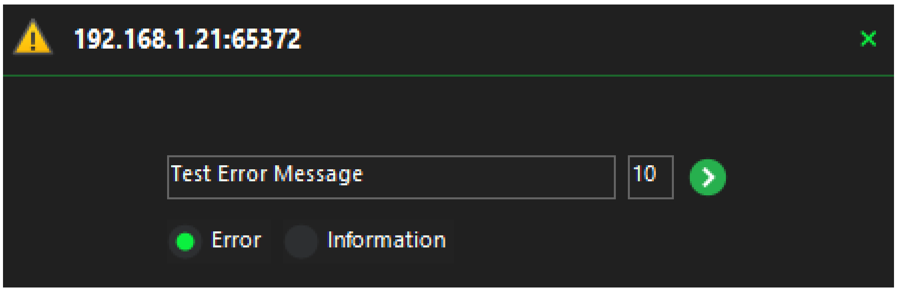
(01:24:10) Server: Hey There
(01:24:16) Client: Hello

With this option, you can chat with the target system. The chat window appears on the target system as shown below (it's not closable, and does not appear in the taskbar), and when you close the chat from the server side, it also closes on the target system:



(01:24:10) Server: Hey There
(01:24:16) Client: Hello

10) Chat (Message Box)



192.168.1.21:65372

Test Error Message

10

● Error ○ Information

This option prompts a message on the target system using the selected box type (information or error). The number on the right indicates how many times this message box will be displayed at once (Maximum 99 at once).

11) Power (Shutdown or Restart)

This option allows you to restart or shut down the target system. If you didn't activate the persistence feature when creating your agent, once the computer restarts or shuts down, the connection will not be reestablished.

12) Kill

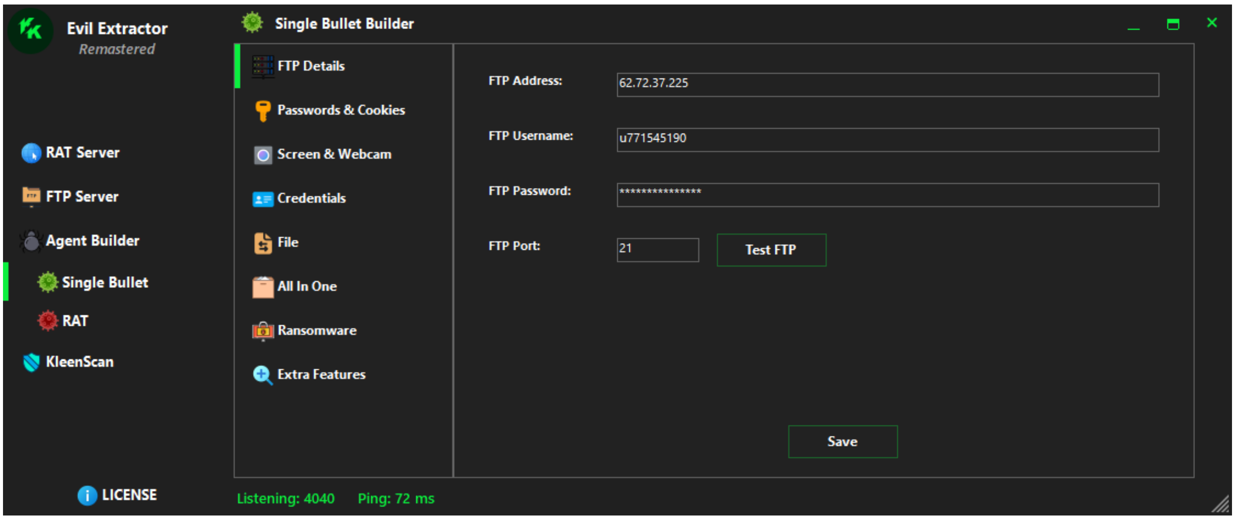
The last option terminates the connection between you and the target system. It cleans up the traces it leaves behind (for example: if you've used the execute file feature to upload and run a file on the other side, it will delete the file if it's no longer in use). If you activated the self-destruction feature when creating your agent, clicking 'kill' will cause your agent to self-destruct after clearing its traces.

Note: If you activated the persistence feature when creating your agent, clicking 'kill' will also remove the persistence feature.

Overview

(Single Bullet)

1) FTP Details



FTP Address: 62.72.37.225

FTP Username: u771545190

FTP Password: ***************

FTP Port: 21

Listening: 4040 Ping: 72 ms

Before we start, you have to set your FTP credentials in "FTP Details" section:

1) FTP Address (mydomain.com or X.X.X.X, it's required)

2) FTP Username (required)

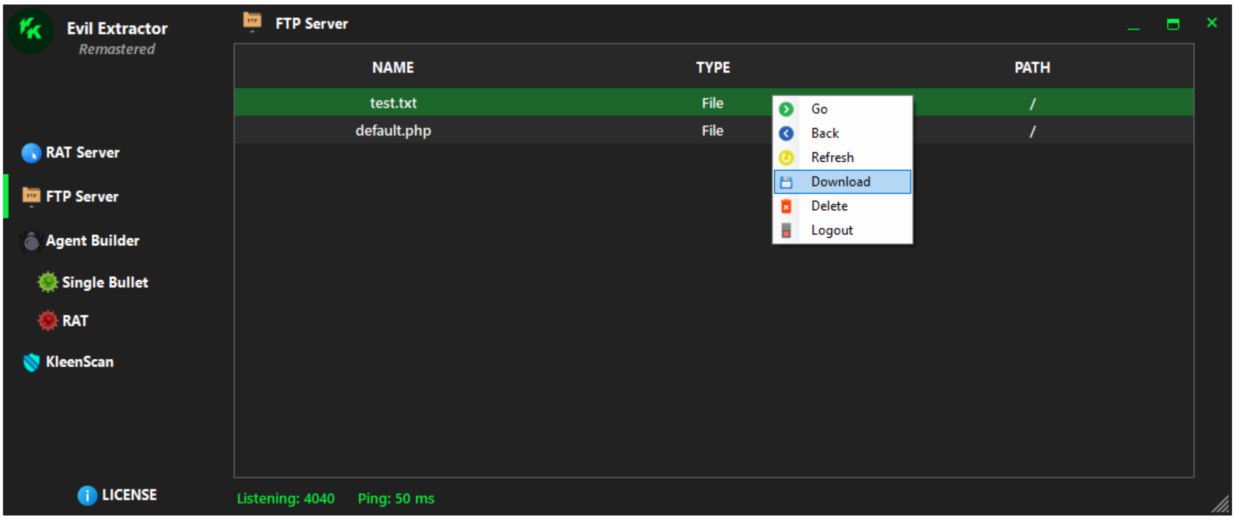
3) FTP Password (required)

4) FTP Port (required), it's usually 21

After setting these parameters, click "Save" button, then you can click "Test FTP" button to make sure that you've entered your credentials correctly (Test FTP button will upload a file named "test.txt" to the root directory of your FTP server).

Your FTP agents are using SSL/TLS (1.2) certificate to protect your FTP credentials. That means, you have to use SSL/TLS certificate on your web hosting/website, it also needs to support SSL/TLS 1.2. Otherwise, your agents can't upload any data to your FTP server.

Note: Just don't forget to get SSL/TLS certificate to your website/web server if you are going to use any other FTP server in the future (after your free FTP server is expired).

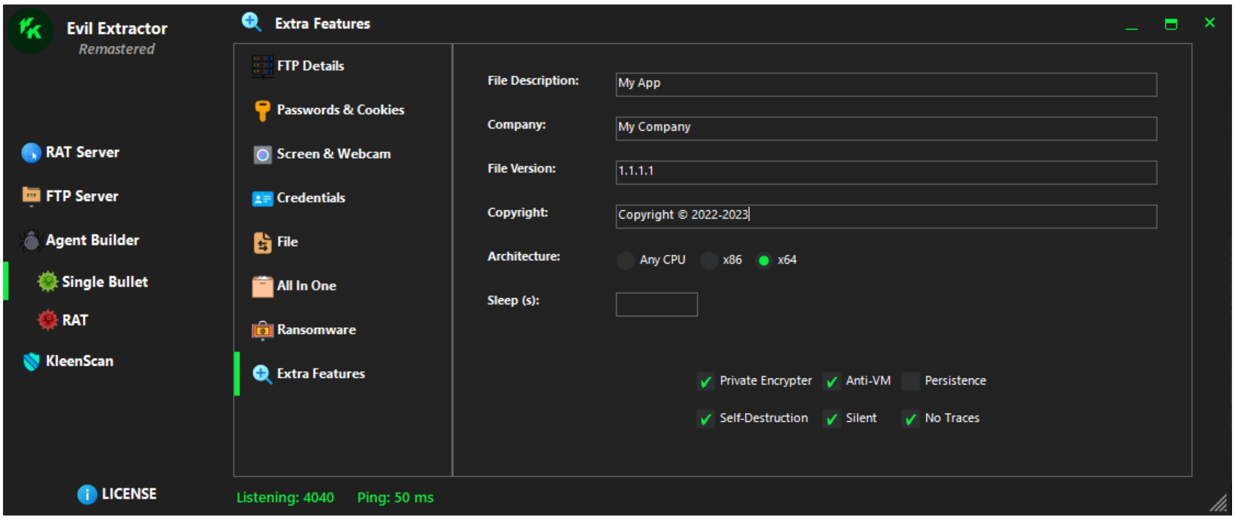


NAME	TYPE	PATH
test.txt	File	/
default.php	File	/

Listening: 4040   Ping: 50 ms

As you can see, test.txt has been successfully uploaded to your FTP Server. FTP Section enables you to delete files, download them (to your local computer), and navigate between folders on the FTP Server. You can use FileZilla or similar service if you don't want to use our FTP Server section.

2) Extra Features



File Description: My App

Company: My Company

File Version: 1.1.1.1

Copyright: Copyright © 2022-2023

Architecture: ○ Any CPU ○ x86 ● x64

Sleep (s):

☑ Private Encrypter ☑ Anti-VM □ Persistence

☑ Self-Destruction ☑ Silent ☑ No Traces

Listening: 4040   Ping: 50 ms

Before creating your Single Bullet Agent, you can take a look at "Extra Features" section. Your agent will be created referencing this section:

Assembly Configuration:

1) File Description (optional)

2) Company Name (optional)

3) File Version (required)

4) Copyright (optional)

5) Architecture (required)

Other Features:

1) Sleep (optional):

This option determines how many seconds your agent should sleep before executing the main code.

2) Private Encrypter (optional):

This option allows you to encrypt your agent and make the source more complicated (using the AES encryption algorithm). This is solely for safeguarding personal information and the structure of the program.

3) Anti-VM (optional):

This option enables Anti-VM, which means your agent will not work on any virtual machine. Also, if any reverse-engineering tool is running, the agent will not function.

4) Persistence (optional):

This option allows you to make your agent persistence on the target system. It cannot used with self-destruction module.

5) Self-Destruction (optional):

If this option checked, your agent will self-destruct after the execution is completed.

Note: This option will not work with Screen & Webcam Extractor and All In One Extractor.

Explanation: Because, these options using infinite loop to take their actions. In that case, these two methods cannot be self-destructed.

6) Silent (optional):

This option allows you to make your agent fully silent on the target system.

7) No Traces (optional):

This option ensures that your agent does not leave traces on the target system.

3) Single Bullet Features

1) Agent Name (required)

2) Error Message (optional)

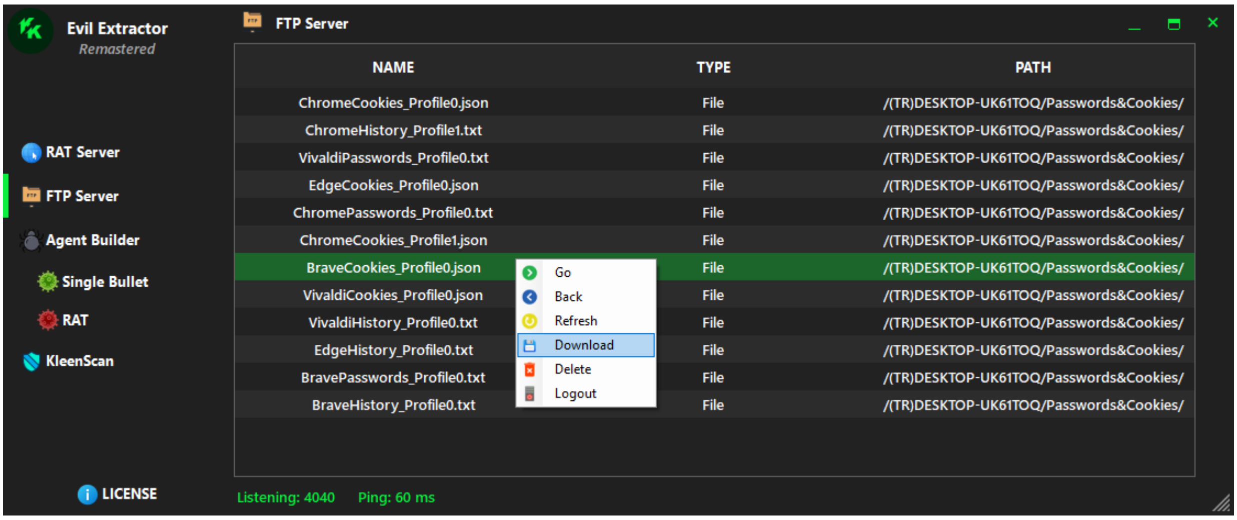
3) Icon Path (optional)

4) Bind Path (optional):

You can bind your agent with the following file types: exe, pdf or image files (jpg or png).

Note: File size is limited with 100 MB. Binder also integrated with persistence module(s). If you bind any file with one of our persistence module(s), your agent will work successfully but additional file will not open at windows startup.

1) Passwords & Cookies Extractor



NAME	TYPE	PATH
ChromeCookies_Profile0.json	File	/(TR)DESKTOP-UK61TOQ/Passwords&Cookies/
ChromeHistory_Profile1.txt	File	/(TR)DESKTOP-UK61TOQ/Passwords&Cookies/
VivaldiPasswords_Profile0.txt	File	/(TR)DESKTOP-UK61TOQ/Passwords&Cookies/
EdgeCookies_Profile0.json	File	/(TR)DESKTOP-UK61TOQ/Passwords&Cookies/
ChromePasswords_Profile0.txt	File	/(TR)DESKTOP-UK61TOQ/Passwords&Cookies/
ChromeCookies_Profile1.json	File	/(TR)DESKTOP-UK61TOQ/Passwords&Cookies/
BraveCookies_Profile0.json	File	/(TR)DESKTOP-UK61TOQ/Passwords&Cookies/
VivaldiCookies_Profile0.json	File	/(TR)DESKTOP-UK61TOQ/Passwords&Cookies/
VivaldiHistory_Profile0.txt	File	/(TR)DESKTOP-UK61TOQ/Passwords&Cookies/
EdgeHistory_Profile0.txt	File	/(TR)DESKTOP-UK61TOQ/Passwords&Cookies/
BravePasswords_Profile0.txt	File	/(TR)DESKTOP-UK61TOQ/Passwords&Cookies/
BraveHistory_Profile0.txt	File	/(TR)DESKTOP-UK61TOQ/Passwords&Cookies/

This option transfers passwords (URL, username, password in ‘txt’ format), cookies (only the necessary ones: Domain, name, value and path in ‘json’ format), and history (URL, title, visits and date in ‘txt’ format) information from supported browsers on the target system to your FTP server.

Additionally, this applies to all profiles; if the target system has multiple profiles, your agent will gather information from all of them.

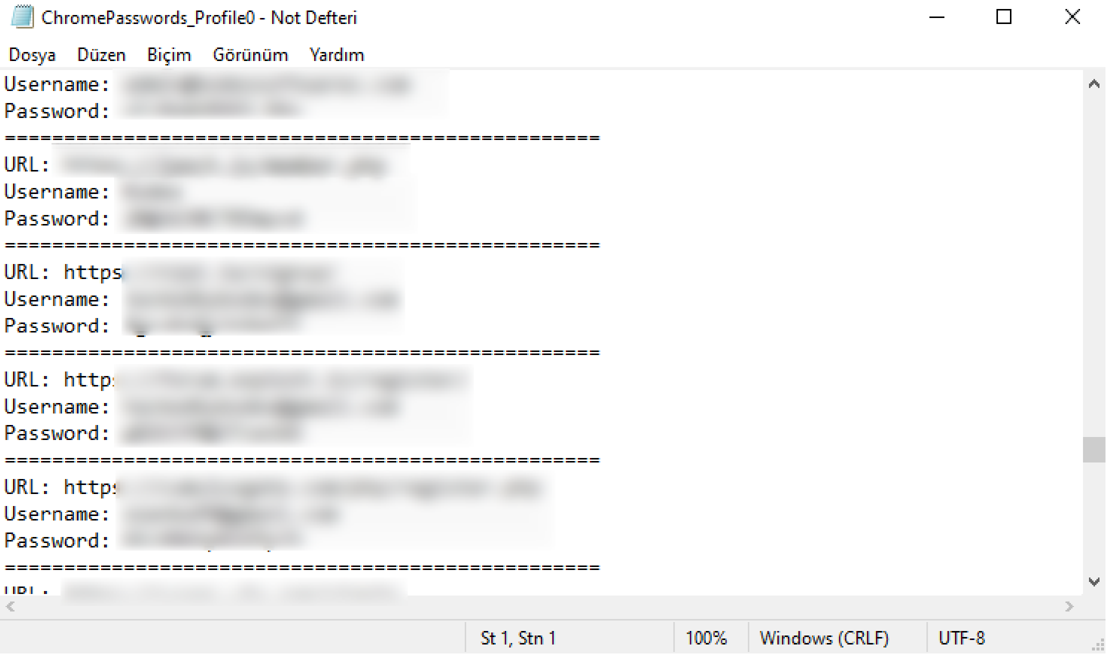
In Chromium v114.x higher browsers, cookie file is locked by default. This means that if the browser is open, access to cookies is not possible. However, this doesn't affect your agent because your agent detects whether access to the cookie file is available; if it's not accessible, it will close the existing browser to gain access to the cookie file.

It will work on chromium v80+ browsers.

Supported browsers:
Chrome, Microsoft Edge, Opera Stable (Default opera browser), Opera GX, Brave, Vivaldi

Default agent size: **4.2 MB**

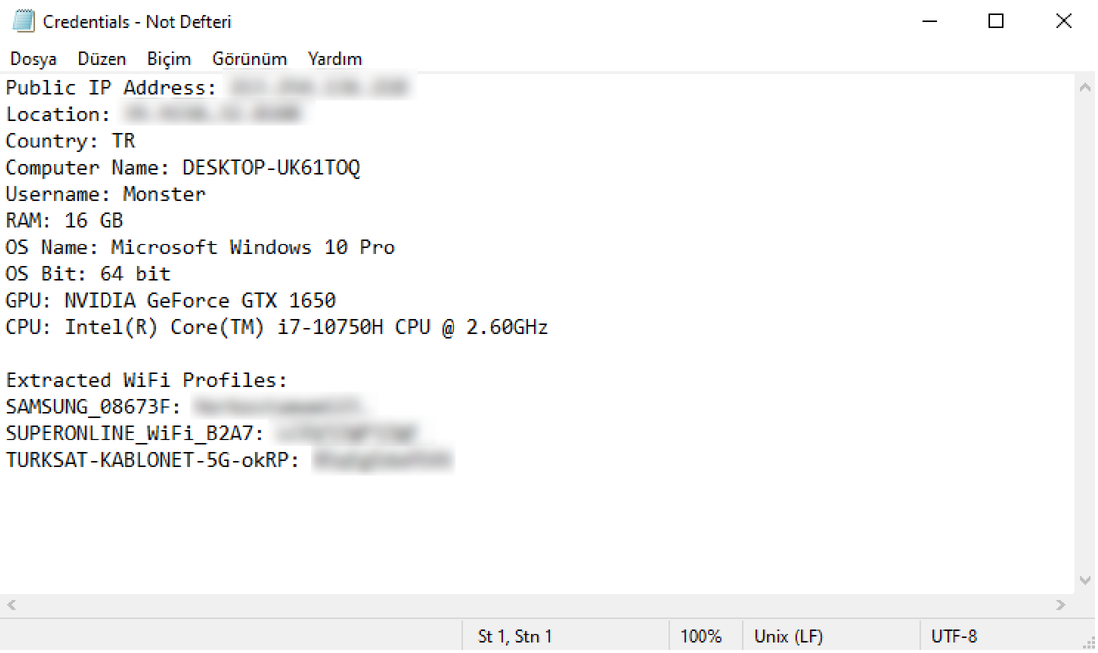
Result:



ChromePasswords_Profile0 - Not Defteri
Dosya Düzen Biçim Görünüm Yardım
St 1, Stn 1
100%
Windows (CRLF)
UTF-8

```
Username: [redacted]
Password: [redacted]
==================================================
URL: [redacted]
Username: [redacted]
Password: [redacted]
==================================================
URL: https[redacted]
Username: [redacted]
Password: [redacted]
==================================================
URL: http[redacted]
Username: [redacted]
Password: [redacted]
==================================================
URL: http[redacted]
Username: [redacted]
Password: [redacted]
==================================================
URL: [redacted]
```

2) Credentials Extractor



```
Public IP Address: [redacted]
Location: [redacted]
Country: TR
Computer Name: DESKTOP-UK61TOQ
Username: Monster
RAM: 16 GB
OS Name: Microsoft Windows 10 Pro
OS Bit: 64 bit
GPU: NVIDIA GeForce GTX 1650
CPU: Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz

Extracted WiFi Profiles:
SAMSUNG_08673F: [redacted]
SUPERONLINE_WiFi_B2A7: [redacted]
TURKSAT-KABLONET-5G-okRP: [redacted]
```

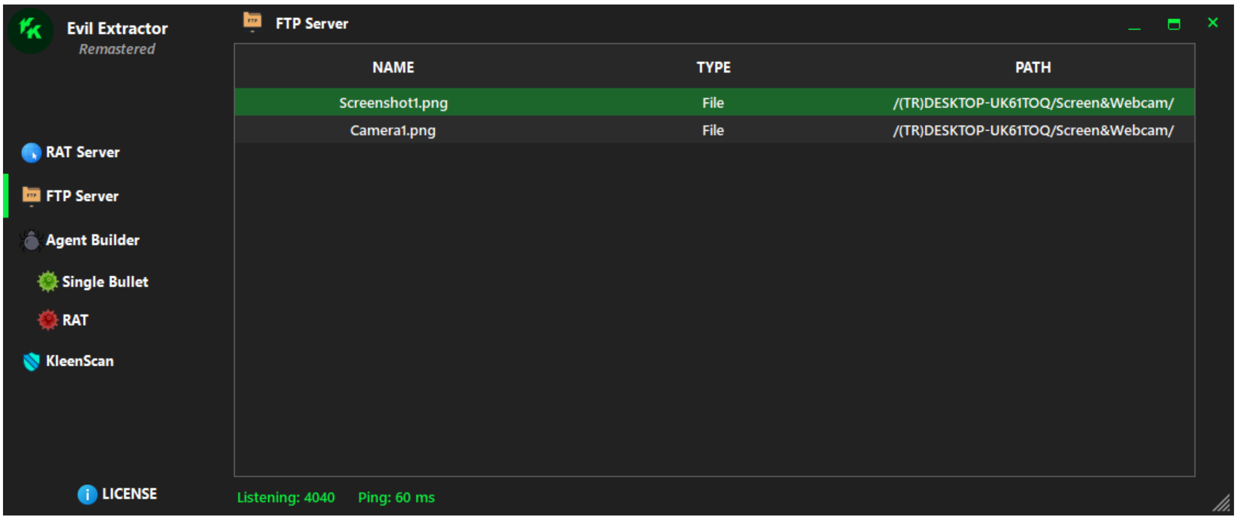
It will bring Public IP Address, Location, Country, Computer Name, Username, RAM, OS Name, OS Bit, GPU, CPU and WIFI Profiles.

Default agent size: 712 KB

3) Screen & Webcam Extractor

Time Range (required):

This option sets how often your agent should send logs to your FTP Server, in minutes.



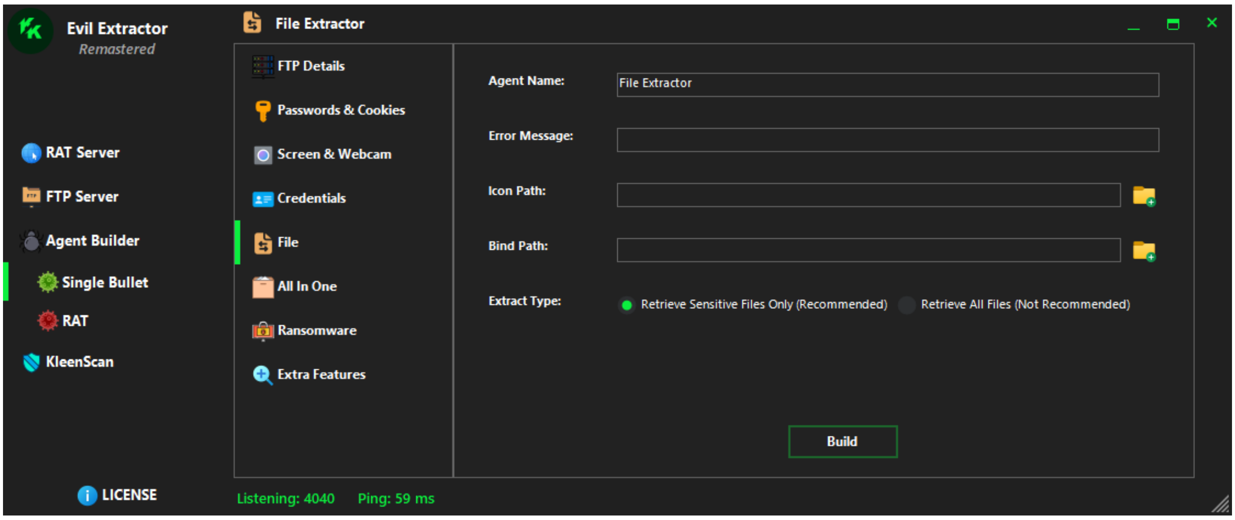
NAME	TYPE	PATH
Screenshot1.png	File	/(TR)DESKTOP-UK61TOQ/Screen&Webcam/
Camera1.png	File	/(TR)DESKTOP-UK61TOQ/Screen&Webcam/

Listening: 4040   Ping: 60 ms

According to the set time range, it will continuously upload screen and camera (if available) images from the target system to your FTP server. Unlike most similar software, it's developed to address screen scaling issues. It will capture the screen seamlessly at various screen resolutions like 100%, 125%, 150%, and so on.

Default agent size: 793 KB

4) File Extractor



Agent Name: File Extractor

Error Message:

Icon Path:

Bind Path:

Extract Type: ● Retrieve Sensitive Files Only (Recommended) ○ Retrieve All Files (Not Recommended)

As you can see, there is two modes available for this method.

1) Retrieve sensitive files only (Recommended)

This option filters the: ".txt, .rtf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .csv" files found in the target system's desktop and downloads folders and <u>matches file names with specific keywords</u> (such as password, account, etc.) and transfers only the files deemed important to your FTP Server.

2) Retrieve all files (Not recommended)

This option transfers all: ".txt, .rtf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .csv, .jpg, .jpeg, .png, .mp4" files found in the target system's desktop and downloads folders to your FTP Server without passing through any filter.

The first option is recommended because FTP servers aren't great for uploading large files; it takes a long time and is unnecessary.

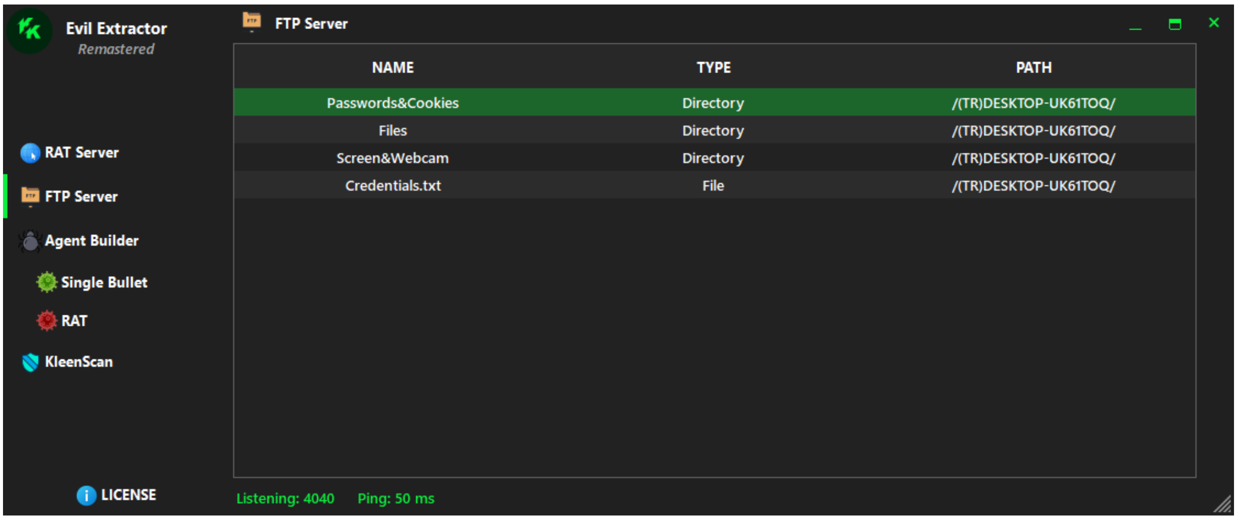
Note: If there are multiple different files with the same name on the target system, the file extractor selects and uploads the newest file to your server. This helps to save time during the upload.

Default agent size: 716 KB

5) All In One Extractor

Time Range (required):

This option sets how often your agent should send logs to your FTP Server, in minutes (it's for Screen & Webcam Extractor).



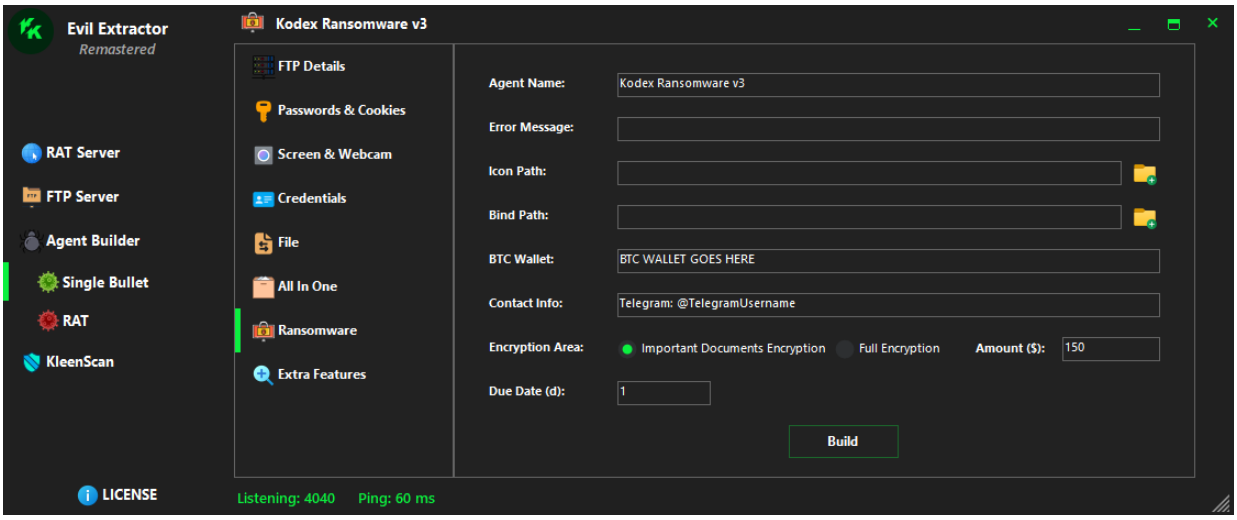
NAME	TYPE	PATH
Passwords&Cookies	Directory	/(TR)DESKTOP-UK61TOQ/
Files	Directory	/(TR)DESKTOP-UK61TOQ/
Screen&Webcam	Directory	/(TR)DESKTOP-UK61TOQ/
Credentials.txt	File	/(TR)DESKTOP-UK61TOQ/

Listening: 4040 Ping: 50 ms

This option combines all other single bullet methods (<u>except for Kodex Ransomware</u>) and allows you to use them all at once. The File Extractor is automatically used in 'Retrieve Sensitive Files Only' mode.

Default agent size: 4.3 MB

6) Kodex Ransomware v3 (Final Form)



Agent Name: Kodex Ransomware v3

Error Message:

Icon Path:

Bind Path:

BTC Wallet: BTC WALLET GOES HERE

Contact Info: Telegram: @TelegramUsername

Encryption Area: ● Important Documents Encryption ○ Full Encryption Amount ($): 150

Due Date (d): 1

The "Remastered" version of Kodex Ransomware uses base64 to encrypt files. In simple terms, it distorts the base64 code of the file according to its own algorithm, and only its algorithm can revert the file to its original state. This is a fairly simple but very difficult-to-crack method. Alongside this algorithm, keys are protected using AES encryption method, consisting of a total of 4 primary keys and 1 decryption key. If any of these keys are missing, decryption cannot be performed in any way.

1) Important Documents Encryption (Recommended)

This option encrypts all files (excluding .exe files), located in the target system’s desktop and downloads folders using a unique encryption algorithm.

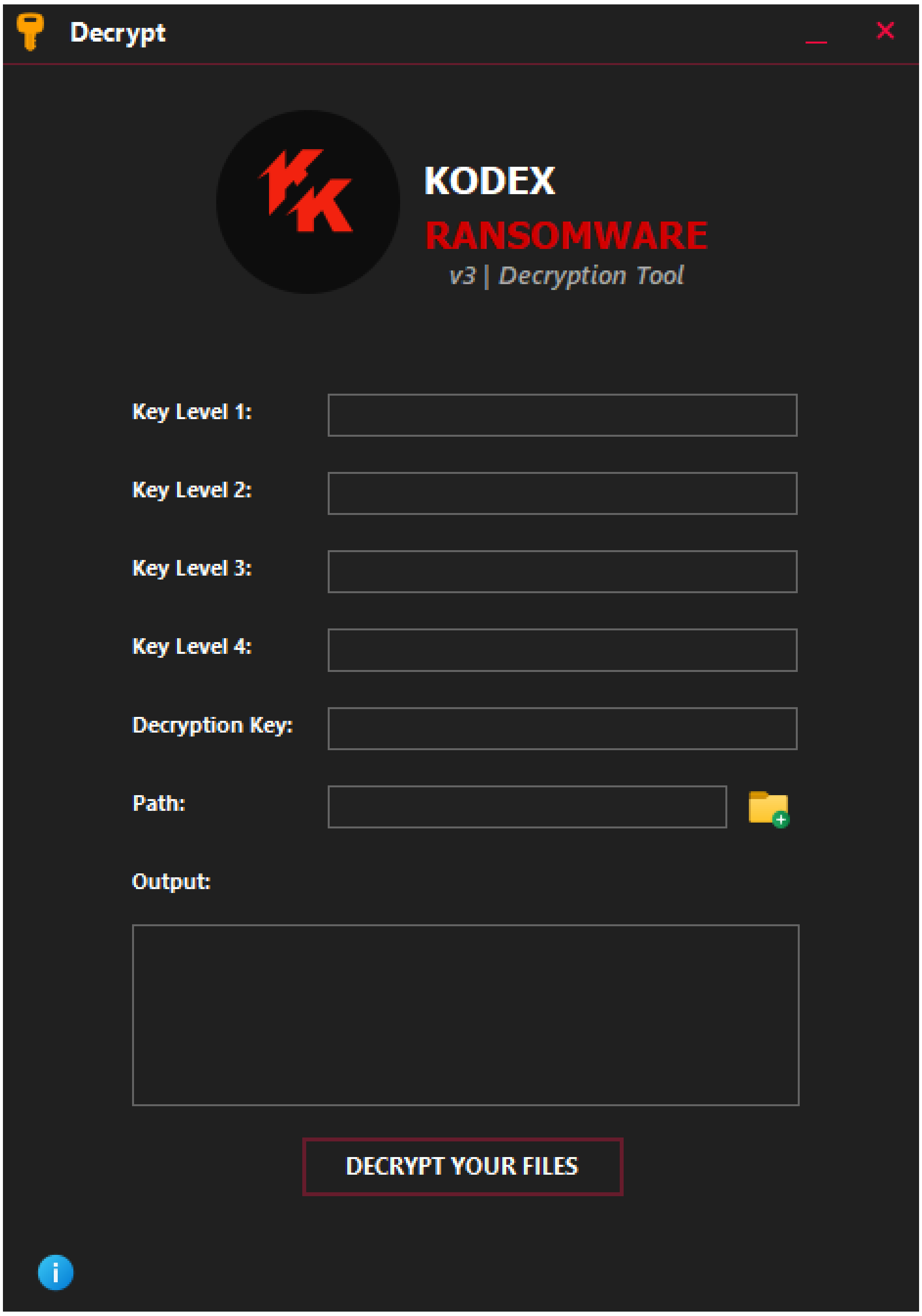
2) Full Encryption

This option encrypts all files (excluding .exe files), located in the target system’s desktop/downloads and other disks (D:\, E:\, F:\, etc.) using a unique encryption algorithm (Except main disk).

Note: Ensure that you haven't selected the persistence feature while using this method (it’s pointless).

WARNING: Please ensure to store your decryption keys securely after creating your ransomware agent. If you lose your decryption keys, it will not be possible to recover any files encrypted as a result.

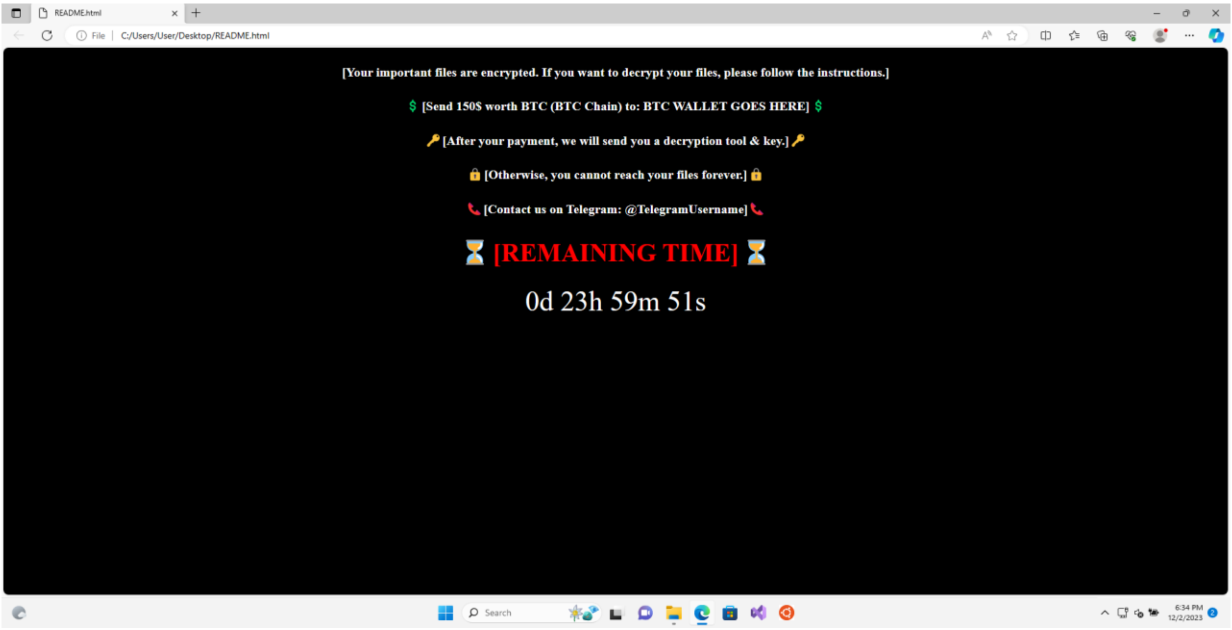
Default agent size: 718 KB



The only way to retrieve encrypted files is by using the 'Kodex Ransomware v3 Decryption Tool'. You can enter the keys found in decryption key.txt into the decryption tool to decrypt the encrypted files. This tool is sent to customers along with Evil Extractor Remastered.

Note: Unlike agents, decryption tool requires .NET Framework 4.8 or higher to run.

Custom Message:



[Your important files are encrypted. If you want to decrypt your files, please follow the instructions.]

💲 [Send 150$ worth BTC (BTC Chain) to: BTC WALLET GOES HERE] 💲

🔑 [After your payment, we will send you a decryption tool & key.] 🔑

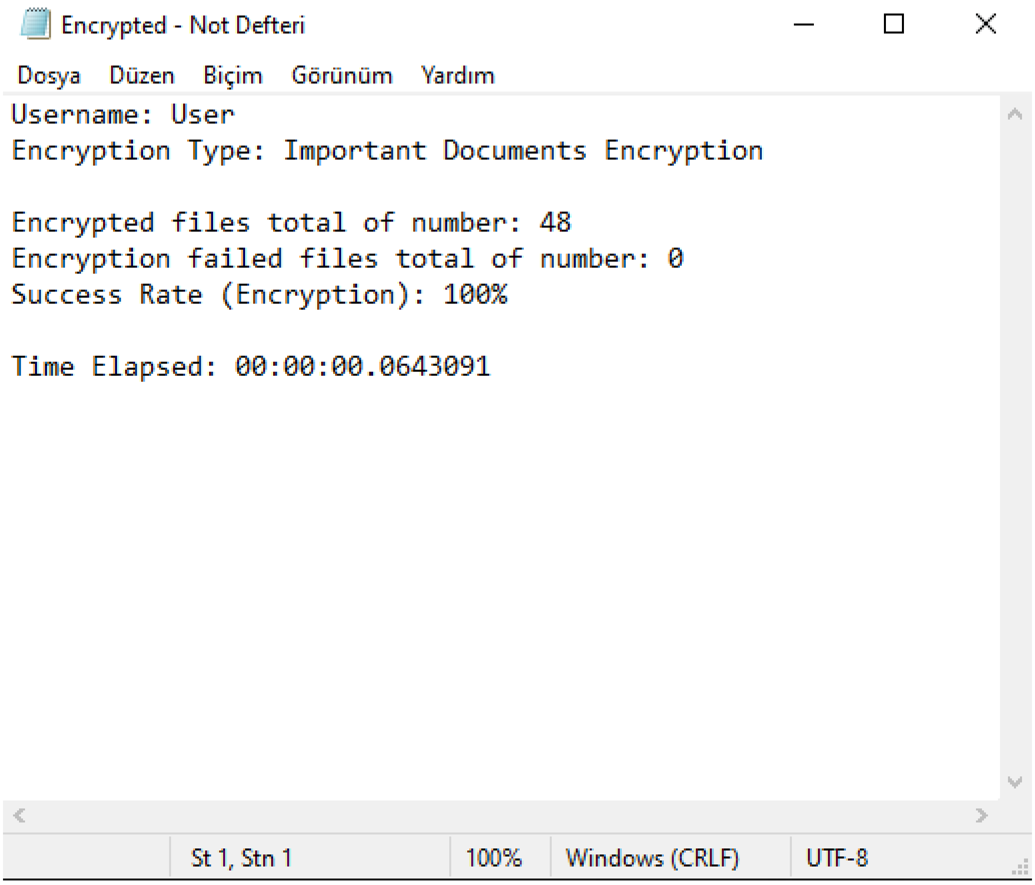
🔒 [Otherwise, you cannot reach your files forever.] 🔒

📞 [Contact us on Telegram: @TelegramUsername] 📞

⏳ [REMAINING TIME] ⏳

0d 23h 59m 51s

Result:

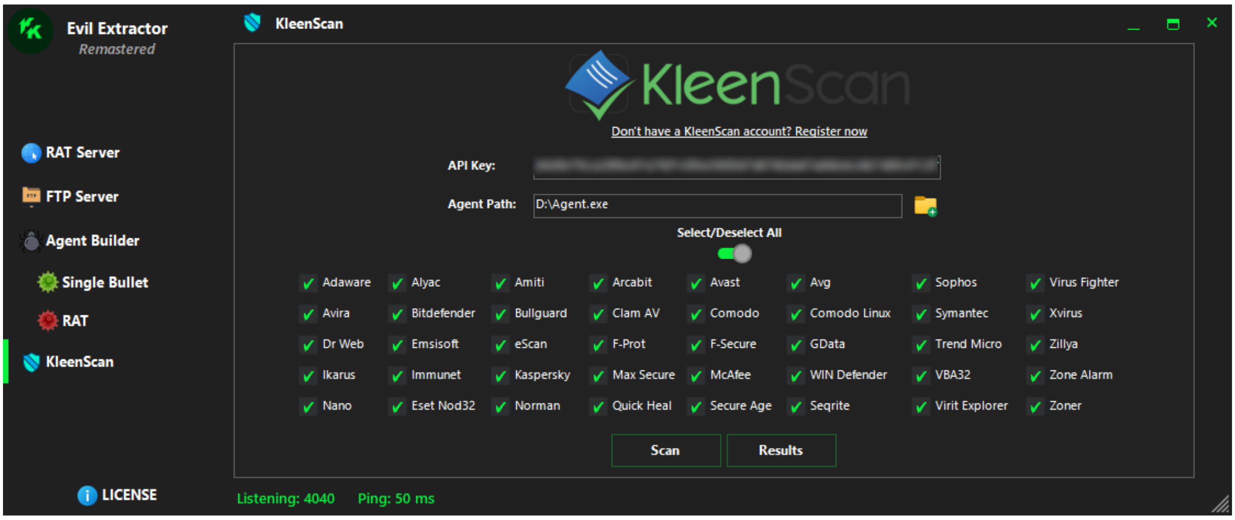


```
Username: User
Encryption Type: Important Documents Encryption

Encrypted files total of number: 48
Encryption failed files total of number: 0
Success Rate (Encryption): 100%

Time Elapsed: 00:00:00.0643091
```

It will upload the results to your FTP Server: Username, Encryption Type, Encrypted files total of number, Encryption failed files total of number, Success Rate and Time Elapsed.

7) KleenScan Service

We integrated KleenScan service to Evil Extractor Remastered. If you want to test your agents' detection value, you can use our Agent Scan system:



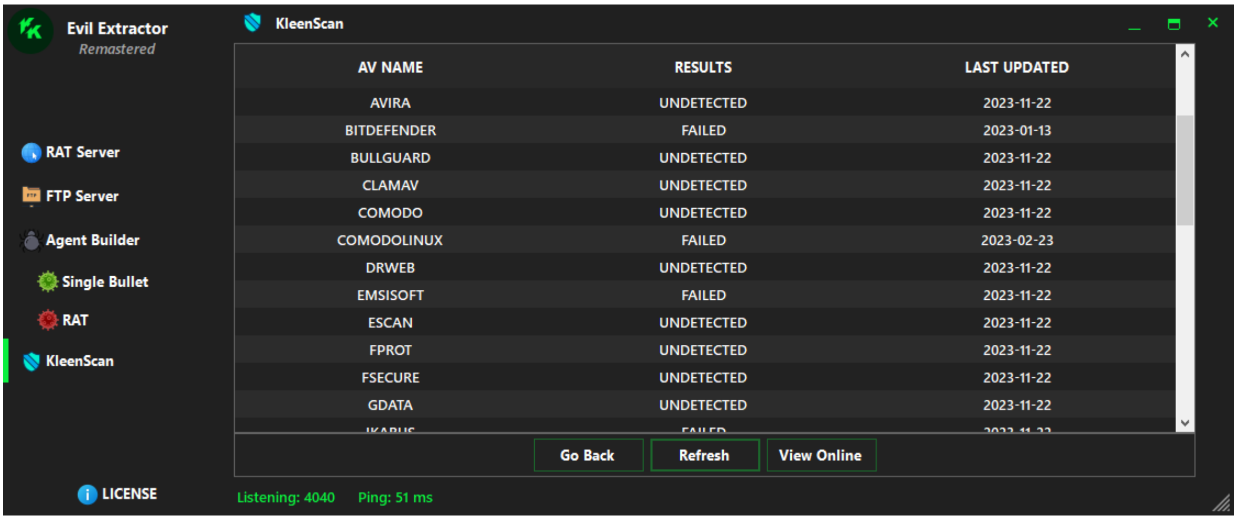
API Key: [redacted]

Agent Path: D:\Agent.exe

☑ Adaware ☑ Avira ☑ Dr Web ☑ Ikarus ☑ Nano
☑ Alyac ☑ Bitdefender ☑ Emsisoft ☑ Immunet ☑ Eset Nod32
☑ Amiti ☑ Bullguard ☑ eScan ☑ Kaspersky ☑ Norman
☑ Arcabit ☑ Clam AV ☑ F-Prot ☑ Max Secure ☑ Quick Heal
☑ Avast ☑ Comodo ☑ F-Secure ☑ McAfee ☑ Secure Age
☑ Avg ☑ Comodo Linux ☑ GData ☑ WIN Defender ☑ Seqrite
☑ Sophos ☑ Symantec ☑ Trend Micro ☑ VBA32 ☑ Virit Explorer
☑ Virus Fighter ☑ Xvirus ☑ Zillya ☑ Zone Alarm ☑ Zoner

Listening: 4040 Ping: 50 ms

The results are as follows:



AV NAME	RESULTS	LAST UPDATED
AVIRA	UNDETECTED	2023-11-22
BITDEFENDER	FAILED	2023-01-13
BULLGUARD	UNDETECTED	2023-11-22
CLAMAV	UNDETECTED	2023-11-22
COMODO	UNDETECTED	2023-11-22
COMODOLINUX	FAILED	2023-02-23
DRWEB	UNDETECTED	2023-11-22
EMSISOFT	FAILED	2023-11-22
ESCAN	UNDETECTED	2023-11-22
FPROT	UNDETECTED	2023-11-22
FSECURE	UNDETECTED	2023-11-22
GDATA	UNDETECTED	2023-11-22
IKARUS	FAILED	2023-11-22

Listening: 4040 Ping: 51 ms