



- 1 INTRODUÇÃO
  - 1.1 BSD License
  - 1.2 O que é “Oblivion”?
  - 1.3 Funcionalidades
  - 1.4 APIs utilizadas
- 2 Compatibilidades
- 3 Oblivion Client
  - 3.1 Instalação
    - 3.1.1 Windows
    - 3.1.2 Linux
  - 3.2 Configuração
    - 3.2.1 APIs
    - 3.2.2 G-Mail
      - 3.2.2.1 Ativar notificações
      - 3.2.2.2 Configurando destinatários
      - 3.2.2.3 Mensagem de notificação
        - 3.2.2.3.1 Mensagem com resultados
    - 3.2.3 Google Drive
      - 3.2.3.1 Alterando pasta destino
    - 3.2.4 Telegram
      - 3.2.4.1 Criando Bot
      - 3.2.4.2 Configurando Bot
      - 3.2.4.3 Habilitar notificação
      - 3.2.4.4 Configurando destinatários
      - 3.2.4.5 Mensagem de notificação
        - 3.2.4.5.1 Mensagem com resultados
    - 3.2.5 Chave de criptografia

- 3.3 Análise
  - 3.3.1 Configurando credenciais
    - 3.3.1.1 Banco de dados
  - 3.3.2 Configurando análise
    - 3.3.2.1 Módulos
    - 3.3.2.2 Formatos
    - 3.3.2.3 Enviando para o Google Drive
  - 3.3.3 Resultados
- 3.4 Histórico
  - 3.4.1 Apagar histórico
- 3.5 Agendamento de análises
- 3.6 Descriptografar
- 4 Oblivion Server
  - 4.1 Instalação
    - Windows 4.1.1
    - Linux 4.1.2
  - 4.2 Configuração
    - 4.2.1 Geral
      - 4.2.1.1 Secret Key
      - 4.2.1.2 APIs
        - 4.2.1.2.1 Ativando APIs
    - 4.2.2 G-Mail
      - 4.2.2.1 Ativar notificações
      - 4.2.2.2 Configurando destinatários
      - 4.2.2.3 Mensagem de notificação
    - 4.2.3 Google Drive
    - 4.2.4 Telegram
      - 4.2.4.1 Ativar notificações
      - 4.2.4.2 Configurando destinatários
      - 4.2.4.3 Mensagem de notificação
    - 4.2.5 SSH
      - 4.2.5.1 SSH ec2
    - 4.2.6 AWS S3
    - 4.2.7 Banco de dados

- 4.3 Requisição
  - 4.3.1 URL
    - 4.3.1.1 Exemplos
  - 4.3.2 Header
    - 4.3.2.1 Exemplos

### 1.1 BSD 3-Clause License

Copyright (c) 2020, Gustavo Torroni  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## 1.2 O que é “Oblivion”?

Oblivion é uma ferramenta open-source feita em Python, que possui funcionalidade de armazenar dados do usuário (senhas, e-mails, domínios, URLs, IPs, CIDRs, Carteira Bitcoin, IPFS hashes etc) e monitorar se esses dados foram vazados.

Comporta uma versão gráfica para desktops, voltada para usuários finais e uma versão servidor, que possui funcionalidades de API.

## 1.3 Funcionalidades

### Common Website

Realiza Web Scraper em sites mais prováveis de divulgarem algum tipo de vazamento de dados.

Sites indexados:

- Pastebin

### Google Dorks

Através de Web Scraper o Oblivion realiza consultas no Google Search utilizando Google Dorks para verificar pastes de vazamentos de dados recentes.

### Word Lists

Realiza Web Scraper em algumas word lists hospedadas no servidor da GitHub e avalia se alguma senha do usuário está contida nelas.

### APIs

Verifica a existência de algum vazamento relacionado com as credenciais do usuário através do consumo de três APIs (Intelx, Scylla e Have I Been Pwned).

### CVEs (experimental)

Consome a Circl CVE API para verificar as últimas 30 CVEs publicadas e analisar se algum softwares presente dentro do host está vulnerável a estas CVEs.

## 1.4 APIs utilizadas

- Scylla – gratuita (<https://scylla.sh/>)
- Intelx – paga (<https://intelx.io/>)
- Have I Been Pwned – paga (<https://haveibeenpwned.com/>)
- Circl CVE Search– gratuita (<https://www.circl.lu/>)

## Compatibilidade -----

As versões citadas abaixo garantem uma estabilidade maior do Oblivion. O usuário pode fazer o uso de outras versões de Python/OS, porém a estabilidade não é garantida:

### Python

- ✓ 3.8.6

### Sistemas operacionais

- ✓ Windows N10 1909
- ✓ Ubuntu Server 20.04 LTS

Alguns sistemas operacionais podem apresentar um certo delay na hora do processamento de chamadas de APIs ou envio de resultados por SSH:

- Windows Server 2019
- Windows Server 2016

# Oblivion Client -----

## 3.1 Instalação

Recomenda-se a instalação 3.8.6 do Python anteriormente a instalação do Oblivion:

(<https://www.python.org/downloads/release/python-386/>)

### 3.1.1 Windows

1. Faça o Download do repositório Oblivion no GitHub (<https://github.com/loseys/Oblivion>)
2. Renomeie a pasta “Windows” para “Oblivion”
3. Acesse a pasta “Windows” e execute o arquivo “install.py”.
4. Execute o arquivo OblivionClient.py

### 3.1.2 Linux

1. \$ git clone <https://github.com/loseys/Oblivion>
2. \$ mv Linux Oblivion
3. \$ cd Oblivion
4. \$ sudo python3.8 install.py
5. \$ sudo python3.8 OblivionClient.py


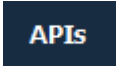
## 3.2. Configuração

As configurações do Oblivion Client se aplicam tanto para o sistema Windows como para o sistema Linux.

**IMPORTANTE:** É essencial que para toda configuração feita o Oblivion seja reiniciado o aplicativo, caso contrário as configurações novas não serão utilizadas.

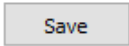


### 3.2.1 APIs

1. Clique no ícone de engrenagem 
2. Clique em “APIs” no canto esquerdo 
3. Coloque as chaves das APIs correspondentes

Keys

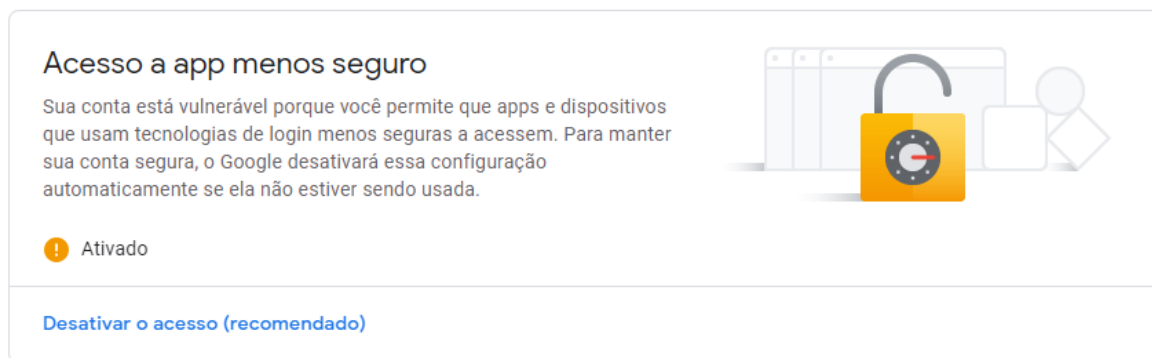
<input type="checkbox"/> Intelx	<input type="text"/>
<input type="checkbox"/> Have I Pwned	<input type="text"/>
<input type="checkbox"/> Scylla	<input type="text"/>

4. Caso queria deixar a API ativa você devera marcar a Check Box referente a API ☐
5. Clique em “save” 

### 3.2.2 G-Mail

É recomendado que seja utilizado uma conta própria para o envio dos avisos, evite o uso de G-Mails pessoais. Também é importante ressaltar que a verificação em duas etapas deve estar obrigatoriamente desativada.

1. Você deve primeiramente ativar a opção “Acesso a app menos seguro” nas opções de segurança do seu G-Mail (<https://myaccount.google.com/lesssecureapps>). É import




#### ← Acesso a app menos seguro

Alguns apps e dispositivos usam tecnologias de login menos seguras, o que deixa sua conta vulnerável. Você pode desativar o acesso desses apps, o que recomendamos, ou ativá-lo se optar por usá-los apesar dos riscos. O Google desativará essa configuração automaticamente se ela não estiver sendo usada. [Saiba mais](#)

Permitir aplicativos menos seguros: ATIVADA



2. Clique no ícone de engrenagem 
3. Clique em “Authentication” no canto esquerdo
4. Introduza o email e a senha da sua conta gmail

Authentication

G-Mail

G-mail

Pass

Authenticate

Before authenticate your g-mail account you need to allow devices third-hand in the settings of your g-mail.



5. Clique em “Authenticate”

6. Clique em “save”



Save

- 7.

### 3.2.2.1 Habilitando notificação

1. Vá em configurações 
2. Clique em “Notification” na esquerda 
3. Para habilitar marque a opção “Notify by e-mail” ☒ Notify by e-mail

### 3.2.2.2 Configurando destinatários

1. Vá em configurações 
2. Clique em “Notification” na esquerda 
3. Digite no campo em branco os e-mails, devem estar separados por “;” e com





The image shows three sequential screenshots of the 'E-mail' configuration form. Each form has a title 'E-mail' and two checkboxes: 'Notify by e-mail' (checked) and 'Send scan result by e-mail (not secure)' (unchecked). The text input field on the right shows the progression of adding email addresses.

- First screenshot:** The input field is empty.
- Second screenshot:** The input field contains the text: `jacare@outlook.com; macaco@outlook.com; leao@outlook.com;`
- Third screenshot:** The input field contains the text: `jacare@outlook.com; macaco@outlook.com; leao@outlook.com;`. A red circle highlights the semicolon at the end of the last email address.

4. É importante que no final contenha “;” para indicar o fim dos e-mails, caso contrario o Oblivion poderá apresentar problemas durante o envio dos e-mails

### 3.2.2.3 Mensagem de notificação

1. Vá em configurações 
2. Clique em “Notification” na esquerda 
3. No campo “E-mail” terá um campo de texto com um código HTML. Para alterar a mensagem você deverá alterar esse código HTML. Caso não tenha familiaridade com HTML recomendamos não alterar o código, apenas a mensagem, para não desencadear problemas no envio do e-mail.

E-mail

☒ Notify by e-mail

☐ Send scan result by e-mail (not secure)



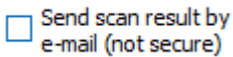
jacare@outlook.com; macaco@outlook.com; leao@outlook.com;

`<h1 style="color: #5e9ca0;"><span style="color: #003366;">Oblivion</span></h1>  
<h4 style="color: #2e6c80;"><span style="color: #ff0000;">Aten&ccedil;&atilde;o:</span></h4>  
<p>Suas cred&ecirc;nciais podem estar em risco: acesse seu aplicativo Oblivion ou <a href="https://drive.google.com/drive/folders/1Zsnh9_79r3hCdGiHeV_sZWkVwckGPzv">clique aqui</a> para saber mais.</p>  
<p>Caso esteja com algum problema, contate o administrador.</p>  
<p>&nbsp;</p>`

**IMPORTANTE:** Não é recomendado o uso de acentos dentro do corpo HTML.

#### 3.2.2.3.1 Mensagem com resultado da análise


Caso queira que o e-mail venha com os resultados no campo da mensagem você deverá:

1. Vá em configurações 
2. Clique em “Notification” na esquerda 
3. No campo “E-mail” marque a opção “Send scan result by e-mail” 

**IMPORTANTE:** Resultados de análises muito longos podem apresentar problema na hora do envio, devido a limitação de caracteres do corpo do e-mail. Aconselha-se evitar o uso desta opção.

### 3.2.3 Google Drive

1. Entre no Google Developer (<https://developers.google.com/drive>)

2. Acesse a aba “Guides” 

3. Clique em “Python” no menu da esquerda

4. Vá em “Enable Drive API”



You're all set!

You're ready to start developing!

5. Clique em “Download cliente configuration” na tela final



6. Salve o arquivo e renomeie para “client\_secret.json”

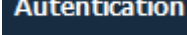
7. Jogue na raiz da pasta do Oblivion

8. Vá no seu Google Drive e crie uma pasta com nome qualquer e acesse ela

9. Copie o ID da pasta contida na URL

 [https://drive.google.com/drive/folders/1Zsnh9\\_79r3hCdGiHeV\\_sZWWhKVwckGPzv](https://drive.google.com/drive/folders/1Zsnh9_79r3hCdGiHeV_sZWWhKVwckGPzv)

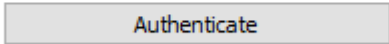
10. Vá no menu de configuração do oblivion 

11. Clique em “Authentication” no canto esquerdo 

12. cole o ID no campo “ID folder”

Google Drive

ID folder



Before authenticate your Google Drive you need to activate the API of your Google Drive account and put the token in root folder of Oblivion.

13. Clique em “Authenticate”

14. Uma página do google irá abrir e você deverá logar com sua conta do Google Drive

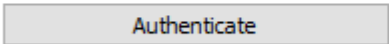
15. Caso apareça uma tela intitulada “Este app não foi verificado”: clique em “avançado” e “Acessar Quickstart”

16. Vá novamente no menu de configuração do Oblivion

17. coloque o ID da pasta do Google Drive e clique em “Authenticate”

Google Drive


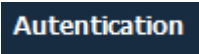
ID folder



Before authenticate your Google Drive you need to activate the API of your Google Drive account and put the token in root folder of Oblivion.

Após isso devesse conter na raiz do seu Google Drive um arquivo com nome de “Authentication.txt”. Este arquivo pode ser excluído sem problemas.

### 3.2.3.1 Alterando pasta destino

1. Vá no menu de configuração do oblivion 
2. Clique em “Authentication” no canto esquerdo 
3. No campo “ID folder” coloque o ID da pasta do Google Drive desejada

Google Drive

ID folder

Before authenticate your Google Drive you need to activate the API of your Google Drive account and put the token in root folder of Oblivion.

4. Clique em “Authenticate”

5. Clique em “save”


### 3.2.4 Telegram

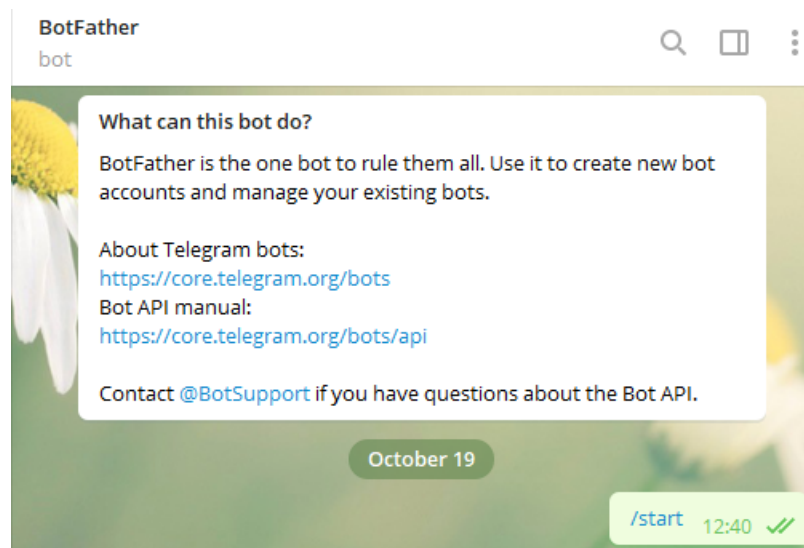
O Bot do Telegram é feito a partir do BotFather e não possui nenhum tipo de custo.

#### 3.2.4.1 Criando Bot

1. Va no Telegram e procure por BotFather




2. O BotFather oficial terá o símbolo de verificado  ao lado do nome
3. Digite no chat “/start”



4. Digite “/newbot”
5. Após isso digite o nome do seu bot (não pode existir nenhum bot com o mesmo nome)
6. Por final o BotFather irá responder com o Token do seu bot, é importante que você mantenha esse Token salvo em um lugar seguro (não compartilhe o Token com ninguém)

Use this token to access the HTTP API:  
**1353559052:AAH\_XE32VQf**  
Keep your token secure and store it safely, it can be used by anyone to control your bot.

### 3.2.4.2 Configurando Bot

1. Vá em configurações 
2. Digite o Token do seu Bot em “Telegram bot”

Others

☒ Telegram bot

3. Após isso clique em “save”

Save

4. Vá em “Authentication”
5. Digite seu Token em “API Bot”

Authentication

Telegram

API bot

Authenticate

Before authenticate your Telegram bot you need to send a message to bot.


6. Clique em “Authenticate”

7. Após isso clique em “save”


Save

8. Vá no campo de pesquisa do Telegram e digite o nome do seu Bot

Global search results

 **Oblivion**  
@xOblivion\_bot

9. Selecione o bot e clique na opção “START”



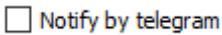


10. Após isso envie qualquer mensagem.

**IMPORTANTE:** O seu Bot do Telegram só ira notificar os usuários que clicaram em “START” e enviaram alguma mensagem para ele.

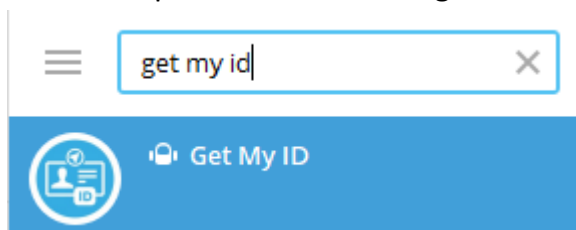


### 3.2.4.3 Habilitar notificação

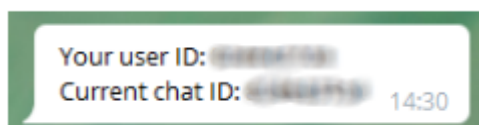
1. Vá em configurações 
2. Clique em “Notification” 
3. Na parte “Telegram” marque a opção “Send scan result by Telegram” ☐ 


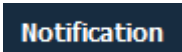
### 3.2.4.4 Configurando destinatários

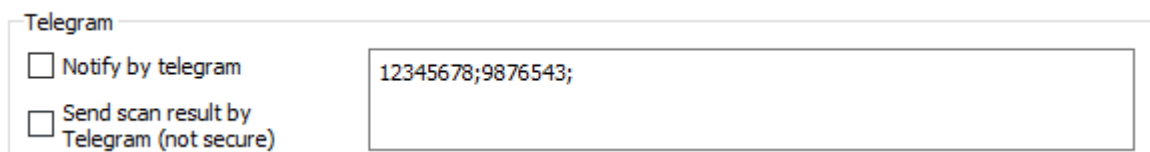
1. Vá no campo de busca do Telegram



2. Digite “get my id” e selecione o primeiro resultado
3. Envie “get my id” no chat
4. O bot irá enviar dois IDs, copie o “Your current ID”




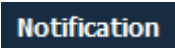
5. Vá em configuração 
6. Clique em “Notification” no canto esquerdo 
7. Em “Telegram” digite no campo à esquerda as IDs destinatários. É importante que os IDs estejam separados por “;” e no final dos IDs esteja contido “;”, caso contrário o Oblivion poderá apresentar problemas no envio da notificação por Telegram.

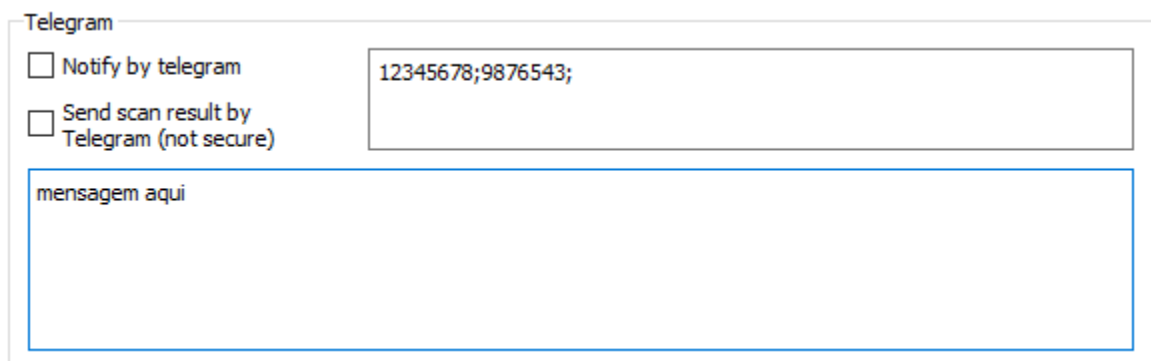
A screenshot of the Telegram notification settings form. The form has a title 'Telegram' and two checkboxes: 'Notify by telegram' and 'Send scan result by Telegram (not secure)'. To the right of the checkboxes is a text input field containing the text '12345678;9876543;'.

Telegram	
<input type="checkbox"/> Notify by telegram	12345678;9876543;
<input type="checkbox"/> Send scan result by Telegram (not secure)	

O envio de avisos pelo Bot telegrama é feito através do ID da conta Telegram do usuário.

### 3.2.4.5 Mensagem de notificação



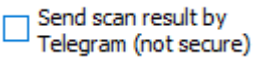
1. Vá em configuração 
2. Clique em “Notification” no canto esquerdo 
3. Na área “Telegram” digite no campo em branco a mensagem desejada



**IMPORTANTE:** Não é recomendado o uso de acentos na mensagem

#### 3.2.4.5.1 Mensagem com resultados

Para notificar os IDs do Telegram com os resultados das análises feitas:

1. Vá em configuração 
2. Clique em “Notification” no canto esquerdo 
3. Na parte “Telegram” marque a opção “ Send scan result by Telegram” 

**IMPORTANTE:** Resultados de análises muito longos podem apresentar problema na hora do envio, devido a limitação de caracteres do corpo da mensagem. Aconselha-se evitar o uso desta opção.

### 3.2.5 Chave de criptografia

Por padrão o Oblivion criptografa o arquivo com uma chave padrão, é altamente recomendável a alteração dessa chave:

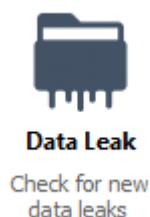
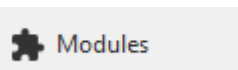
1. Acesse a raiz da pasta do Oblivion
2. Acesse a pasta “etc”
3. Abra o arquivo “key\_crypt.txt”
4. Apague a chave padrão e escreva uma nova chave, sem o uso de espaços

**IMPORTANTE:** Caso apresente algum tipo de problema com a nova chave escrita, escreva uma nova chave mantendo os caracteres especiais e alterando apenas as letras e os números da chave padrão, mantendo o as letras maiúsculas e as maiúsculas.

## 3.3 Análise

### 3.3.1 Configurando credenciais

1. Vá em módulos no canto esquerdo
2. Clique em “Data Leak”



3. Irá abrir uma tela para colocar as credenciais
4. Clique em alguma célula e digite a credencial
5. Após isso clique em “save”

#### Passwords

Coluna dos senhas.

#### E-mails

Coluna dos e-mails

#### Documents

Será a coluna onde o usuário irá colocar qualquer tipo de dado que não seja uma senha ou um e-mail, por exemplo um endereço de IP, um domínio etc.

### 3.3.1.1 Banco de dados

O Oblivion utiliza um banco de dados “.db”, ele se localiza na raiz da pasta do Oblivion. É importante que o arquivo de banco de dados esteja com o nome de “data.db”.

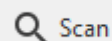
Todo o processamento de dados é feito através do SQLite.

O formato do banco de dados se consiste em:

- Data (Table)
  - email TEXT (column)
  - senha TEXT (column)
  - documento TEXT (column)

### 3.3.2 Configurando análise

Em “scan” localizado na esquerda você poderá ter acesso a parte de scan

A screenshot of the Oblivion configuration window. The window has three tabs: "Configurations", "Modules", and "Format". The "Configurations" tab is active. It contains two sections: "Scan" and "Completion". In the "Scan" section, there is a "Delay scan(s)" input field with the value "3,00" and a "Loop scan" checkbox. In the "Completion" section, there are two checkboxes: "Close after conclude" and "Turn off after conclude".

Section	Option	Value / State
Scan	Delay scan(s)	3,00
	Loop scan	<input type="checkbox"/>
Completion	Close after conclude	<input type="checkbox"/>
	Turn off after conclude	<input type="checkbox"/>

**Delay scan(s):** tempo entre da análise no modo loop

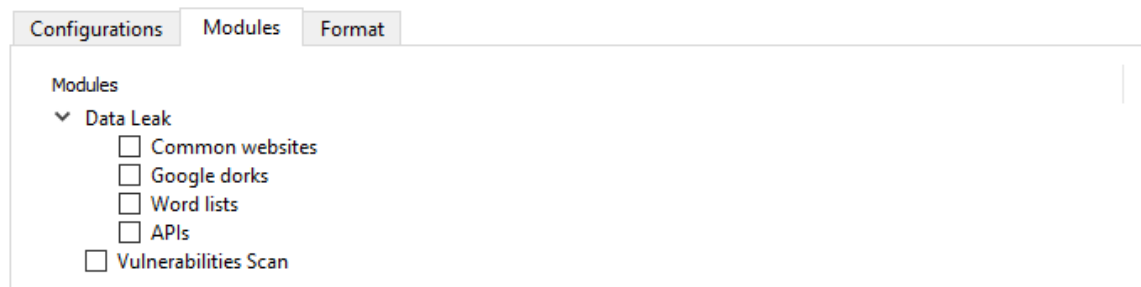
**Loop scan:** ativar análise em modo loop, onde o Oblivion irá ficar scaneando até achar alguma credencial vazada.

**Close after conclude:** fechar o Oblivion após a conclusão da análise

**Turn off after conclude:** desligar o Oblivion após concluir a análise

### 3.3.2.1 Módulos

Clicando em “modules” você terá acesso à área de módulos e funcionalidades:



Para maiores informações sobre os módulos acesse o item 1.3.

### 3.3.2.2 Formatos

Caso o Oblivion detecte algum vazamento das credenciais ele irá gerar um arquivo com o relatório. Os tipos de arquivos suportados são:

- ✓ .txt
- ✓ .docx
- ✓ .pdf
- ✓ .xlsx
- ✓ .json
- ✓ .html
- ✓ .xml
- ✓ .db

Para gerar o arquivo desejado você deverá marcar a checkbox responsável.

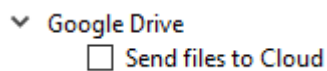
**Raw data (.txt):** gerar dado bruto

**Occult password:** ocultar final das senhas com asterísticos

**Encrypt:** gerar o arquivo de forma criptografada

### 3.3.2.3 Enviando para Google Drive

Para fazer o envio dos resultados automaticamente para o Google Drive marque a opção “Send file to Cloud”.



### 3.3.3 Resultados

Todos os arquivos com os resultados estão na pasta “Oblivion” dentro da pasta Documentos.

## 3.4 Histórico

Em “History” no canto esquerdo  terá todas as análises realizadas pelo Oblivion.

### 3.4.1 Apagar o histórico

Abra o arquivo “Oblivion\etc\logs\activity.txt” e apague todo o conteúdo. É importante que não delete este arquivo.

### 3.5 Agendamento de análises

O agendamento de análise é feito pelo Windows Scheduler na versão do Oblivion Windows e pelo Crontab na versão do Oblivion Linux.

Para agendar uma análise clique em “Schedule” no canto esquerdo  **Schedule**.

1. Selecione a data e o horário

Date:

Time:

2. Digite o nome da análise

Date:

Time:

3. Selecione os parâmetros (para mais detalhes acesse os itens 3.3.2, 3.3.2.1, 3.3.2.2 e 3.3.2.3)

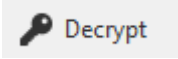
Results


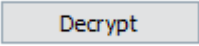
- ▼ Modules
  - ☐ Vulnerabilities Scan
  - ▼ Data Leak
    - ☐ Common websites
    - ☐ Google dorks
    - ☐ Word lists
    - ☐ APIs
  - ▼ Generate results
    - ▼ Local file
      - ☐ Raw data (.txt)
        - > ☐ .txt
        - > ☐ .docx
        - > ☐ .pdf
        - > ☐ .xlsx
        - > ☐ .json
        - > ☐ .html
        - > ☐ .xml
        - > ☐ .db
    - ▼ Google Drive

4. Clique em “create”

Create

### 3.6 Descriptografar

No canto esquerdo clique em “Decrypt” .

1. Caso esteja recebendo uma arquivo criptografado com uma chave diferente você deverá colocar a chave no campo “Key” (para saber mais sobre a chave de criptografia veja o item 3.2.5)
2. Digite o caminho do item no campo “path” ou clique em  e selecione o arquivo
3. Clique em 



# Oblivion Server -----

## 4.1 Instalação

Recomenda-se a instalação 3.8.6 do Python anteriormente a instalação do Oblivion:

(<https://www.python.org/downloads/release/python-386/>)

### 4.1.1 Windows

1. Faça o Download do repositório Oblivion no GitHub (<https://github.com/loseys/Oblivion>)
2. Renomeie a pasta “Windows” para “Oblivion”
3. Acesse a pasta “Windows” e execute o arquivo “install.py”.
4. Execute o arquivo OblivionServer.py

### 4.1.2 Instalação Linux

6. \$ git clone <https://github.com/loseys/Oblivion>
7. \$ mv Linux Oblivion
8. \$ cd Oblivion
9. \$ sudo python3.8 install.py
10. \$ sudo python3.8 OblivionServer.py

## 4.2 Configuração

### 4.2.1 Geral

Para acessar as configurações gerais do servidor acesse:

“/Oblivion/etc/serverx/config/config\_server.py”

**api\_return:** ativar ou desativar o retorno do json após realizar uma requisição para o servidor Oblivion

**db\_name\_f:** nome do arquivo de database que o servidor irá utilizar, este arquivo se localiza na raiz da pasta do Oblivion

**situacaoIntelx:** ativa ou desativa o uso da API IntelX no Oblivion servidor

**situacaoHaveIPwned:** ativa ou desativa o uso da API Have I Been Pwned no Oblivion servidor

**situacaoScylla:** ativa ou desativa o uso da API Scylla no Oblivion servidor

**id\_f3:** e-mail de notificação

**id\_f4:** senha do e-mail de notificação

Para alterar a porta de funcionamento de Oblivon acesse o arquivo “/Oblivion/OblivionServer.py” e altere a linha 314:

```
if __name__ == "__main__":  
    app.run(host='0.0.0.0', port="5000")
```

(imagem da linha 314 do arquivo “/Oblivion/OblivionServer.py”)

Para deixar o server funcionando localmente exclua o “host='0.0.0.0'”:

```
if __name__ == "__main__":  
    app.run(port="5000")
```

(imagem da linha 314 do arquivo “/Oblivion/OblivionServer.py”)

### 4.2.1.1 Secret Key

Para fazer qualquer tipo de requisição para o Oblivion Server será necessário passar uma chave de segurança na URL ou nos Headers:

localhost:5000/oblivion/<secret key>/<parametros>

“Key”: “<secret key>”

Acessando o arquivo “/Oblivion/etc/serverx/config/keys.txt” você poderá adicionar a chave de segurança. É interessante que a chave de segurança possua strings maiúsculas, strings minúsculas, letras e caracteres por motivos de segurança.

Inicialmente cada chave será associada com um cliente. Além disso é importante que cada chave seja colocada em uma linha diferente, seguindo o exemplo a seguir:



```
GNU nano 4.8 keys.txt
8dAMM9sPfJDRhDYA9xgqC4Fk3Ks1D
kNS$1w01ncAL2ns1fMC012Awqxqw0
$e0ns1IX5Ns8KSz1%1gPakOPQW1C@
```

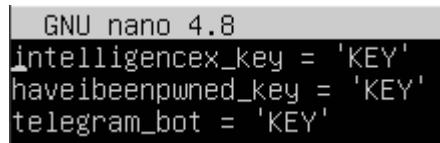
(imagem do arquivo “/Oblivion/etc/serverx/config/keys.txt”)

### 4.2.1.2 APIs

Para configurar as chaves das APIs primeiramente você deverá acessar:

“/Oblivion/etc/api/keys\_db.txt”

Dentro do arquivo você deverá substituir “KEY” pela sua chave da API, mantendo as aspas simples no início e no fim da chave



```
GNU nano 4.8
intelligencex_key = 'KEY'
haveibeenpwned_key = 'KEY'
telegram_bot = 'KEY'
```

(imagem do arquivo “/Oblivion/etc/api/keys\_db.txt”)

#### 4.2.1.2.1 Ativando APIs

Acessando “Oblivion/etc/serverx/config/config\_server.py” você poderá definir quais APIs serão utilizadas pelo servidor. No campo “/API” você poderá escolher entre “False” para desativar o uso da API e “True” para ativar o uso da API.

```
# /APIs
# Enables or disables the API.
situacaoIntelx = False
situacaoHaveIPwned = False
situacaoScylla = True
```

(imagem do arquivo “/Oblivion/etc/serverx/config/config\_server.py”)

#### 4.2.2 G-Mail

Você deve primeiramente ativar a opção “Acesso a app menos seguro” nas opções de segurança do seu G-Mail (<https://myaccount.google.com/lesssecureapps>).



(imagem com a opção “Acesso a app menos seguro” ativa)

##### 4.2.2.1 Ativar notificações

Acessando “Oblivion/etc/parameters.txt” você poderá ativar a notificação simples e a personalizada. Para ativar ou desativar basta trocar de “no” para “yes”.

```
GNU nano 4.8
email_notification:no
email_body:no
telegram_notification:no
telegram_body:no
```

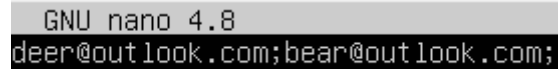
(imagem do arquivo “/Oblivion/etc/parameters.txt”)

**email\_notification:** ativar ou desativar o envio de notificação por e-mail

**email\_body:** ativar ou desativar o envio de notificação com os resultados da análise no corpo da mensagem

#### 4.2.2.2 Configurando destinatário

Em “/Oblivion/etc/notification/email/emails.txt” você poderá adicionar os e-mails que deseja notificar. Entre cada e-mail deverá conter “;” como separador. Após o último e-mail é necessária que tenha “;”.



```
GNU nano 4.8  
deer@outlook.com;bear@outlook.com;
```

(imagem do arquivo “/Oblivion/etc/email/emails.txt”)

#### 4.2.2.3 Mensagem de notificação

Para alterar a mensagem de notificação vá para “/Oblivion/etc/notification/email/body.html”. A mensagem será enviada em forma de HTML.



```
GNU nano 4.8 body.html Modified  
<h1 style="color: #5e9ca0;"><span style="color: #003366;">Oblivion</span></h1>  
<h4 style="color: #2e6c80;"><span style="color: #ff0000;">Aten&cedil;&atilde;o:</span></h4>  
<p>Suas cred&ecirc;ncias podem estar em risco: acesse seu aplicativo Oblivion ou <a href="https://>  
<p>Caso esteja com algum problema contate o administrador.</p>  
<p>&nbsp;</p>
```

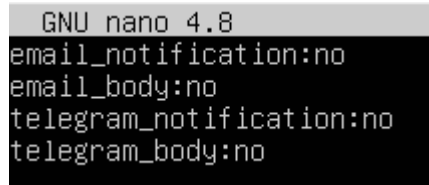
(imagem do arquivo “/Oblivion/etc/email/body.html”)

#### 4.2.4 Telegram

Para saber mais sobre a criação de um bot para Telegram acesse o item 3.2.4.1.

#### 4.2.4.1 Ativar notificações

No arquivo “/Oblivion/etc/parameters.txt/” você encontrara o seguinte conteúdo:



```
GNU nano 4.8
email_notification:no
email_body:no
telegram_notification:no
telegram_body:no
```

(imagem do arquivo “/Oblivion/etc/parameters.txt/”)

**telegram\_notification:** ativar ou desativar a notificação por Telegram

**telegram\_body:** ativar ou desativar o envio dos resultados das análises por mensagem

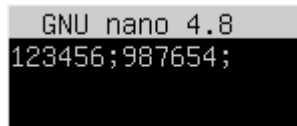
Para ativar ou desativar você deverá alterar de “no” para “yes”.

#### 4.2.4.2 Configurando destinatários

Em “/Oblivion/etc/notification/users.txt” você poderá adicionar as IDs das contas Telegram que serão notificadas. Importante ressaltar que apenas colocar o número da conta Telegram não funcionará, necessita ser o ID da conta.

Para saber como adquirir o ID da conta Telegram acesse o item 3.2.4.4.

Cada ID Telegram deve ser separado por “;”. No final de todos os IDs deverá conter um “;”.



```
GNU nano 4.8
123456;987654;
```

(imagem do arquivo “/Oblivion/etc/notification/users.txt”)

#### 4.2.4.3 Mensagem de notificação

No arquivo “/Oblivion/etc/notification/message.txt” você poderá alterar a mensagem de notificação do Telegram. Não é recomendado o uso de acentos nas letras.



```
GNU nano 4.8                                message.txt
Atencao: suas credenciais podem estar em risco: acesse seu aplicativo Oblivion ou clique aqui (http
```

(imagem do arquivo “/Oblivion/etc/notification/message.txt”)

## 4.2.5 SSH

Para adicionar um caminho SSH vá para “/Oblivion/etc/serverx/config/ssh\_hosts.txt”.

Syntax:

IP;PORTA;LOGIN;SENHA;PASTA\_DESTINO;SECRET\_KEY

Cada caminho SSH deverá obrigatoriamente ter uma Secret Key associada a ele, para saber mais sobre Secret Key veja o item 4.2.1.1

```
GNU nano 4.8 ssh_hosts.txt
192.168.15.24;22;oblivion;123;/home/oblivion;key
4.145.200.23;22;test;123;/home/test;key
```

(imagem do arquivo “/Oblivion/etc/serverx/config/ssh\_hosts.txt”)

**IMPORTANTE:** Caso os resultados não estejam sendo enviados para a pasta destino use o home do usuário, por exemplo “/home/test”.

### 4.2.5.1 SSH ec2

Para adicionar um caminho SSH de uma ec2 da AWS é necessário primeiramente que você copie sua chave .pem para o diretório “/Oblivion/etc/serverx/pems”. Após isso abra o arquivo de hosts SSH “/Oblivion/etc/serverx/config/ssh\_hosts.txt”:

Syntax:

DNS\_PUBLICA;PORTA;LOGIN;SENHA;PASTA\_DESTINO;SECRET\_KEY;NAME\_PEM\_FILE

```
GNU nano 4.8 ssh_hosts.txt
ec2-3-83-117-20.compute-1.amazonaws.com;22;ubuntu;123;/home/ubuntu;key;god.pem
ec2-3-86-89-244.compute-1.amazonaws.com;22;ubuntu;123;/home/ubuntu;key;god.pem
```

(imagem do arquivo “/Oblivion/etc/serverx/config/ssh\_hosts.txt”)

No caso da imagem acima a senha foi colocada apenas por uma questão de Syntax, mas não foi necessário.

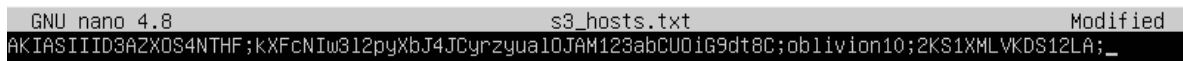
**IMPORTANTE:** É importante que seja utilizado a DNS público da instância ec2. Caso os resultados não estejam sendo enviados para a pasta destino use o home do usuário, por exemplo “/home/test”.

## 4.2.6 AWS S3

Para adicionar um bucket S3 vá para “/Oblivion/etc/serverx/config/s3\_hosts.txt”.

Syntax:

`ACCESS_KEY;SECURITY_KEY;BUCKET_NAME;SECRET_KEY.`



```
GNU nano 4.8 s3_hosts.txt Modified
AKIASIIID3AZXS4NTHF;kXFcNIw812pyXbJ4JCyrzyua10JAM123abCU0iG9dt8C;oblivion10;2KS1XMLVKDS12LA;_

```

(imagem do arquivo “/Oblivion/etc/serverx/config/s3\_hosts.txt”)

Access key: chave de acesso do bucket

Security key: chave de segurança do bucket

Bucket name: nome do bucket

Cada parâmetro deve estar separado por “;” e no final deverá apresentar “;”. É necessário que o cliente tenha uma Secret Key associada, para saber mais sobre a Secret Key acesse o item 4.2.1.1.

## 4.2.7 Banco de dados

O Oblivion utiliza um banco de dados “.db”, ele se localiza na raiz da pasta do Oblivion. É importante que o arquivo de banco de dados esteja com o nome de “data.db”.

Todo o processamento de dados é feito através do SQLite.

O formato do banco de dados se consiste em:

- Data (Table)
  - email TEXT (column)
  - senha TEXT (column)
  - documento TEXT (column)

Você pode optar tanto em gerar um banco de dados com o Oblivion Client quanto criar seu próprio arquivo .db seguindo as tables e as column acima.



## 4.3 Requisição

### 4.3.1 URL

Para fazer uma requisição por URL você deverá seguir a seguinte Syntax:

`x.x.x.x:porta/oblivion/<security key>/<parametros>`

Lista de parâmetros:

- &EM"email@outlook.com" (utiliza um e-mail personalizado, precisa estar com aspas duplas)
- &PW"password123" (utiliza uma senha personalizado, precisa estar com aspas duplas)
- &DM"www.teste.com" (utiliza uma dado personalizado, precisa estar com aspas duplas)
- &%loop (manter análise em loop até encontrar algum data leak)
- &common\_web (utilizar a funcionalidade Common Websites)
- &google\_dorks (utilizar a funcionalidade Google Dorks)
- &wordlists (utilizar a funcionalidade Word List)
- &dado\_bruto (salvar dado bruto dos resultados obtidos)
- &api (utilizar a funcionadade das APIs)
- &<tipo arquivo>\_f (gerar arquivo)
- &<tipo arquivo>\_ocult (gerar arquivo com senhas semi ucultas)
- &<tipo arquivo>\_cript (gerar arquivo criptografado)
- &gdrive (mandar arquivos para o Google Drive)
- &aws\_s3 (mandar arquivos para o s3 da AWS)
- &ssh (enviar arquivos por SSH)

Tipos de arquivos suportados:

- ✓ .txt
- ✓ .docx
- ✓ .pdf
- ✓ .xlsx
- ✓ .json
- ✓ .html
- ✓ .xsl
- ✓ .db

Funcionamento:

txt\_f > gera um arquivo .txt comum

txt\_f + txt\_cript > gera um arquivo .txt criptografado

txt\_f + txt\_cript + txt\_ocult > gera um arquivo .txt criptografado com as senhas ocultas

#### 4.3.1.1 Exemplos

Utilizando a funcionalidade APIs. Gerando um arquivo .txt:

[4.25.192.8:5000/oblivion/DRhDYA9xgqC4Fk3Ks1D/&api&txt\\_f](http://4.25.192.8:5000/oblivion/DRhDYA9xgqC4Fk3Ks1D/&api&txt_f)

Utilizando a funcionalidade Common Websites e a funcionalidade APIs. Gerando os resultados em um .docx criptografado:

[4.25.192.8:5000/oblivion/DRhDYA9xgqC4Fk3Ks1D/&api&common\\_web&docx\\_f&docx\\_cript](http://4.25.192.8:5000/oblivion/DRhDYA9xgqC4Fk3Ks1D/&api&common_web&docx_f&docx_cript)

Utilizando a funcionalidade Word List com uma senha personalizada. Gerando os resultados em um .db:

[4.25.192.8:5000/oblivion/DRhDYA9xgqC4Fk3Ks1D/&wordlists&PW"password123"&db\\_f](http://4.25.192.8:5000/oblivion/DRhDYA9xgqC4Fk3Ks1D/&wordlists&PW\)

Utilizando a funcionalidade APIs. Gerando os resultados em um .html e enviando por SSH e para o bucket S3:

[4.25.192.8:5000/oblivion/DRhDYA9xgqC4Fk3Ks1D/&api&html\\_f&ssh&aws\\_s3](http://4.25.192.8:5000/oblivion/DRhDYA9xgqC4Fk3Ks1D/&api&html_f&ssh&aws_s3)

Utilizando a funcionalidade APIs. Gerando os resultados em um arquivo txt e enviando para o Google Drive:

[4.25.192.8:5000/oblivion/DRhDYA9xgqC4Fk3Ks1D/&api&txt\\_f&gdrive](http://4.25.192.8:5000/oblivion/DRhDYA9xgqC4Fk3Ks1D/&api&txt_f&gdrive)

### 4.3.2 Header

Para fazer uma requisição por URL você deverá seguir a seguinte Syntax:

```
h = {  
    'Key': '<Security_key>',  
    '<parametro>': '<condicao>'  
}  
  
rr = requests.get('http://4.25.192.8:5000/oblivion/api/&', headers=h)  
print(rr.text)
```

Lista de parâmetros:

- '&Em': '{email@outlook.com}' (utiliza um e-mail personalizado, precisa estar com aspas duplas)
- '&Pw': '{password123}' (utiliza uma senha personalizado, precisa estar com aspas duplas)
- '&Dm': '{www.teste.com}' (utiliza uma dado personalizado, precisa estar com aspas duplas)
- 'loop': 'True' (manter análise em loop até encontrar algum data leak)
- 'common\_web': 'True' (utilizar a funcionalidade Common Websites)
- 'google\_dorks': 'True' (utilizar a funcionalidade Google Dorks)
- 'wordlists': 'True' (utilizar a funcionalidade Word List)
- 'dado\_bruto': 'True' (salvar dado bruto dos resultados obtidos)
- 'api': 'True' (utilizar a funcionadade das APIs)
- '<tipo arquivo>\_f': 'True' (gerar arquivo)
- '<tipo arquivo>\_ocult': 'True' (gerar arquivo com senhas semi ucultas)
- '<tipo arquivo>\_cript': 'True' (gerar arquivo criptografado)
- 'gdrive': 'True' (mandar arquivos para o Google Drive)
- 'aws\_s3': 'True' (mandar arquivos para o s3 da AWS)
- 'ssh': 'True' (enviar arquivos por SSH)

Tipos de arquivos suportados:

- ✓ .txt
- ✓ .docx
- ✓ .pdf
- ✓ .xlsx
- ✓ .json
- ✓ .html
- ✓ .xsl
- ✓ .db

Funcionamento:

txt\_f > gera um arquivo .txt comum

txt\_f + txt\_cript > gera um arquivo .txt criptografado

txt\_f + txt\_cript + txt\_ocult > gera um arquivo .txt criptografado com as senhas ocultas

#### 4.3.2.1 Exemplos

Utilizando a funcionalidade APIs. Gerando os resultados em um arquivo pdf e enviado por SSH e para o bucket S3.

```
h = {  
  'Key': 'DRhDYA9xgqC4Fk3Ks1D',  
  'pdf_f': 'True',  
  'api': 'True',  
  'aws_s3': 'True',  
  'ssh': 'True'  
}
```

Utilizando a funcionalidade Common Website com um e-mail personalizado. Gerando os resultados em um arquivo .pdf criptografado

```
h = {  
  'Key': 'DRhDYA9xgqC4Fk3Ks1D',  
  'pdf_f': 'True',  
  'pdf_cript': 'True',  
  'common_web': 'True',  
  '&Em': '{exemplo@gmail.com}'  
}
```