

# Monitorando phishings - Home

Neste laboratório vamos seguir a ideia de **yin yang(bem e o mal)** com o objetivo de ver como os cibercriminosos criam campanhas de phishing e como podemos buscar por elas com algumas técnicas.

## **1. Sobre o autor**

Olá, eu sou o JC GreenMind, atualmente analista de segurança da informação com foco em Threat Intelligence e Purple Team. Sou idealizador do projeto OSINT Village e busco sempre participar de projetos da comunidade.

## 2. Sumário

<b>1. Sobre o autor</b>	<b>2</b>
<b>2. Sumário</b>	<b>3</b>
<b>3. Introdução</b>	<b>8</b>
<b>4. Antes de começar</b>	<b>9</b>
4.1 Qual o objetivo do curso	9
4.2 Profissionais que podem ser beneficiados	9
<b>5. A história das fontes públicas de informação</b>	<b>9</b>
5.1 O início na segunda guerra mundial	9
5.2 OSINT e a ligação com o FBI	9
<b>6. Laboratório exemplo</b>	<b>11</b>
<b>7. Infraestrutura - Montando Lab</b>	<b>11</b>
7.1 A importância da criação de um laboratórios	11
7.1.1 Porque devemos criar um lab?	11
7.1.2 Corromper evidências	11
7.1.3 Sua segurança	12
7.2 Requisitos necessários para a criação do laboratório	12
7.2.1 Recomendações	12
7.2.2 Instalando requisitos laboratório	12
7.5 Instalando Virtualbox - Linux	13
7.5.1 Instalando Virtualbox - DPKG	13
7.5.2 Antes de começar	13
7.5.3 Obtendo o Virtualbox	13
7.5.4 Buscando por outras versões	13
7.5.5 Iniciando a instalação	13
7.6 Instalando Virtualbox - Windows	13
7.7 Instalando Extension Pack	18
7.8 Conhecendo o Genymotion Android	20
7.8.1 O que é o Genymotion?	20
6.8.2 Como ele pode nos ajudar ?	20
6.8.3 Criando conta	20
6.8.4 Instalando Genymotion - Linux	21
6.8.4.1 Realizando download	21
6.8.4.2 Documentação	22
6.8.4.3 Observações	23
6.8.4.4 Comandos para instalação	23
6.8.5 Instalando Genymotion - Windows	25
6.8.5.1 Realizando download	25
6.8.5.2 Iniciando instalação	26

6.8.5.3 Permissão de administrador	26
6.8.5.4 Escolher a língua de Instalação	26
6.8.5.5 Localização	26
6.8.5.6 Nome menu principal	26
6.8.5.7 Shortcut	27
6.8.5.8 Instalando	27
6.9 Criando máquina Kali Oficial - Virtualbox	28
6.9.1 Criando máquina Kali Oficial - Virtualbox	28
6.9.2 O que é o Kali Linux	28
6.9.3 Site oficial	29
6.9.4 Download	29
6.9.5 Verificando ISO	30
6.9.6 Importando máquina	30
6.9.7 Configurando - Rede	32
6.9.8 Alterando usuário	32
6.10 Criando laboratório Android - Genymotion	33
6.10.1 Criando laboratório Android - Genymotion	33
<b>8. Criando lista de visibilidade</b>	<b>37</b>
Criando nossa lista de visibilidade	37
O que é lista de ativos ou lista de visibilidade ?	37
Como podemos nos beneficiar?	37
Quais informações são importantes ?	37
Logo e imagens de produtos	37
URLs (redes sociais)	38
Domínios	38
IPS ou blocos de IPS	39
Aplicativos oficiais	39
Palavras chaves	39
Serviços	40
Criando nossa lista de palavras chaves	40
<b>9. TLDs</b>	<b>40</b>
O que é TLDs?	41
Criando uma lista de TLDs	42
<b>10. Criando domínios</b>	<b>43</b>
Criando domínios gratuitos	43
Dominios .tk	43
Criação de domínio	43
Criando domínios pagos	48
Super Domínios	48
<b>11. Cybersquatting</b>	<b>49</b>
Cybersquatting e Typosquatting diferença	49
Algumas variantes de ataque	49

URL - Adição	49
URL - bitsquatting	49
URL - Dicionário	49
URL - homoglyph	49
URL - omission	50
URL - repetition	50
URL - replacement	51
URL - subdomain	51
URL - tld-swap	51
URL - transposition	51
<b>12. Monitorando domínios e encontrando domínios disponíveis</b>	<b>52</b>
DNSTwist	52
Sobre o projeto	52
Link oficial do Projeto	52
Instalando DNSTwist - source code	52
Instalando DNSTwist - Docker	52
Instalando DNSTwist - Python PIP	52
Como usar DNSTwist	53
Versão web do DNSTwist	53
URLCrazy	53
Instalando URLCrazy	53
Casos de uso	54
Algumas opções de uso	54
phishing_catcher	55
Projeto oficial	55
O que é o phishing_catcher ?	56
Instalando o phishing_catcher	56
Como usar o phishing_catcher?	56
<b>13. Hospedagens</b>	<b>57</b>
Hospedagens gratuitas	57
Hostinger	57
Hospedagens Pagas	58
Digital Ocean	58
AWS	58
<b>14. Configuração de DNS</b>	<b>58</b>
DNS no domínio	58
Cloudflare	58
Outros	59
<b>15. Materiais indexados na internet</b>	<b>60</b>
Motores de busca	60
Google Dorks	60
Palavras chaves e Dorks	60

intitle	60
Operador -site	61
<b>16. Redes sociais</b>	<b>61</b>
Buscando páginas suspeitas	61
namechk	61
Como posso usar o namechk ?	61
Facebook	62
Instagram	63
Twitter	63
Youtube	63
LinkedIn	64
<b>17. Comunidades</b>	<b>65</b>
MISP	66
O que é o MISP	66
Como ele pode nos ajudar ?	66
MISP comunidades	66
MISP feeds	66
Phishingtank	67
Como usar o Phishingtank ?	67
OpenPhish	70
O que é o OpenPhish?	71
Outras comunidades	71
<b>18. Referências</b>	<b>72</b>
Referências - O que é a virtualização	72
## Referências - Virtualbox	72
MISP feeds - Feeds	72
TLD	72

### 3. Introdução

Esse material tem como objetivo compartilhar algumas soluções e técnicas que podemos utilizar para realizar a busca por domínios e páginas de redes sociais que possam estar sendo usados em campanhas de phishing.

Esse material ainda está sendo desenvolvido, então qualquer feedback ou até outra solução que possa nos ajudar nos informe, caso encontre algum erro ou tenha alguma sugestão só me avisar.

## 4. Antes de começar

### 4.1 Qual o objetivo do curso

Esse curso tem o objetivo de dar uma introdução na busca de phishings usando diversas fontes públicas, projetos e soluções que possam auxiliar empresas a realizar as buscas de páginas de phishing.

### 4.2 Profissionais que podem ser beneficiados

Diversos profissionais podem ser beneficiados, profissionais de threat intelligence, analistas de fraudes, analistas de segurança da informação e entusiastas que buscam aprender mais sobre o tema.

## 5. A história das fontes públicas de informação

### 5.1 O início na segunda guerra mundial

A segunda guerra mundial foi um dos maiores marcos da humanidade, foi o maior conflito militar, cerca de 40 milhões de civis e 20 milhões de soldados perderam sua vida durante o conflito. A segunda guerra aconteceu entre **1 de setembro de 1939 até 2 de setembro de 1945**. Na década de 1930 o canal usado era o rádio para buscar informações , atualmente temos navegadores , serviços como redes sociais onde podemos encontrar informações sobre uma pessoa ou até um grupo de pessoas. Atualmente navegando na internet temos a possibilidade de encontrar diversas fontes de informações públicas, sejam elas vindas de algumas fontes e são as:

- Jornais
- Revistas
- Televisão

Tudo começou no **Foreign Broadcast Information Service (FBIS)** esse grupo foi pioneiro no uso de **Open Source Intelligence (OSINT)**, deram início ao projeto na década de **1930** na **Universidade de Princeton**. Durante a segunda guerra mundial ele teve a função de analisar os noticiários por rádio e monitorar publicações oficiais da **União das repúblicas Socialistas Soviéticas**. Informações públicas que poderiam ser usadas a favor dos **Estados Unidos** durante a guerra.

### 5.2 OSINT e a ligação com o FBI

Os ataques de 11 de setembro de 2001 mudaram a história, não só nos Estados Unidos e sim em todo o mundo. Acredito que todas as pessoas têm uma memória do dia, a minha era a terceira série e a professora avisando sobre o ataque e só entendi de fato o que estava acontecendo em casa. Mesmo pequeno não faltou notícias e informações sobre o caso.

Já em 8 de novembro de 2005 foi anunciado por John Negroponte o Open Source Center (OSC) que é um braço da CIA , têm o objetivo de coletar , reunir , trabalhar informações e foi daí que saiu o termo OSINT. Com diversas fontes públicas é possível poupar com custo operacional , porém a quantidade de dados é gigantesca , é necessário o auxílio de pessoas que conheçam sobre o assunto para saber criar filtros para os dados e assim filtrar e gerar informações válidas.

## 6. Laboratório exemplo

Nesse laboratório irei usar o domínio do meu controle chamado:

- badbank.com.br

## 7. Infraestrutura - Montando Lab

### 7.1 A importância da criação de um laboratórios

#### 7.1.1 Porque devemos criar um lab?



Diariamente realizamos análises de phishings, páginas suspeitas e aplicativos. Devido a isso é de suma importância a criação de laboratórios, seja para máquinas virtuais Linux com o Kali, Android com o Genymotion e laboratório windows com máquinas atualizadas.

Algumas páginas só estão disponíveis para Windows, outras para celular e a grande maioria está disponível para todos os sistemas.

Com essa segurança a mais em páginas de phishing, as campanhas são direcionadas apenas para um grupo e assim tendo a possibilidade de adicionar/executar malwares.

### 7.1.2 Corromper evidências

Para uma melhor análise é recomendado que sempre use um laboratório limpo, sem cache e sem estar prejudicado.



### 7.1.3 Sua segurança

É recomendado usar laboratórios via rede NAT, assim evita que caso a máquina host seja comprometida e sua rede.

## 7.2 Requisitos necessários para a criação do laboratório

Esses requisitos são usados para o laboratório de monitoramento de phishing.

### 7.2.1 Recomendações

Recomendamos que usem uma máquina Linux com o sistema operacional que você se sente à vontade, eu uso e recomendo o Ubuntu ou Debian.

Link do Debian:

- <https://www.debian.org/download>

Link do Ubuntu:

- <https://ubuntu.com/download/desktop>

## 7.2.2 Instalando requisitos laboratório

Kali será usado para realizar uma análise com as soluções open source disponíveis e vamos realizar a importação de uma máquina virtual oficial disponível no site do Kali.

Genymotion vai nos auxiliar na análise mobile de páginas suspeitas, já que algumas páginas de phishing só estão disponíveis para o Android.

O Windows será usado para análise de phishing com foco nesse sistema operacional.

## 7.5 Instalando Virtualbox - Linux

### 7.5.1 Instalando Virtualbox - DPKG

- Site oficial: <https://www.virtualbox.org/>
- Link download: <https://www.virtualbox.org/wiki/Downloads>

### 7.5.2 Antes de começar

Nos exemplos eu vou usar o sistema operacional Debian, para acompanhar você precisa estar usando um sistema baseado no **Debian**.

### 7.5.3 Obtendo o Virtualbox

Vamos para o link:

- [https://www.virtualbox.org/wiki/Linux\\_Downloads](https://www.virtualbox.org/wiki/Linux_Downloads)

Nesse caso vou usar o Debian bullseye 64 Bits.

- [http://download.virtualbox.org/virtualbox/6.1.28/virtualbox-6.1\\_6.1.28-147628~Debian~buster\\_amd64.deb](http://download.virtualbox.org/virtualbox/6.1.28/virtualbox-6.1_6.1.28-147628~Debian~buster_amd64.deb)

### 7.5.4 Buscando por outras versões

Caso queira usar uma outra versão antiga podemos usar também o seguinte link:

- <https://download.virtualbox.org/virtualbox/>

### 7.5.5 Iniciando a instalação

Nesse exemplo estou no diretório:

- /home/greenmind/Downloads

Para instalar preciso fazer:

```
sudo dpkg -i virtualbox-6.1_6.1.28-147628~Debian~bullseye_amd64.deb
```

Após isso o Virtualbox vai estar instalado

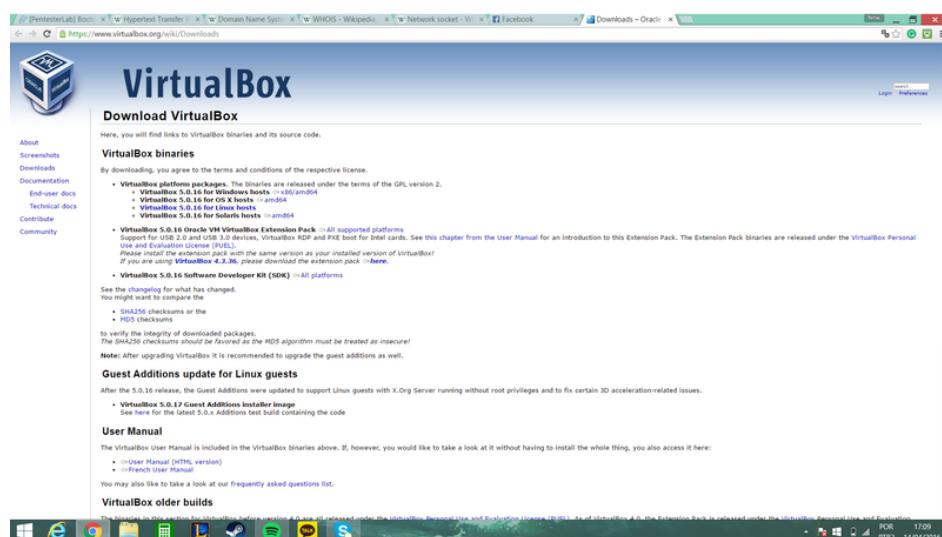
**Menú de aplicativos -> Sistema -> Oracle VM VirtualBox.**

## 7.6 Instalando Virtualbox - Windows

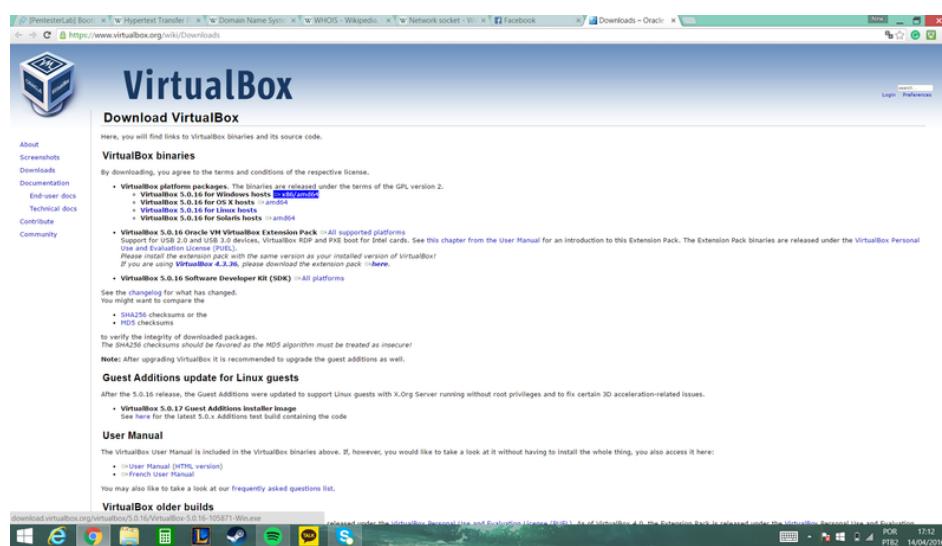
A instalação em um sistema operacional windows é bem fácil.

Vá para o site oficial do VirtualBox no seguinte link como na imagem abaixo.

- <https://www.virtualbox.org/wiki/Downloads>



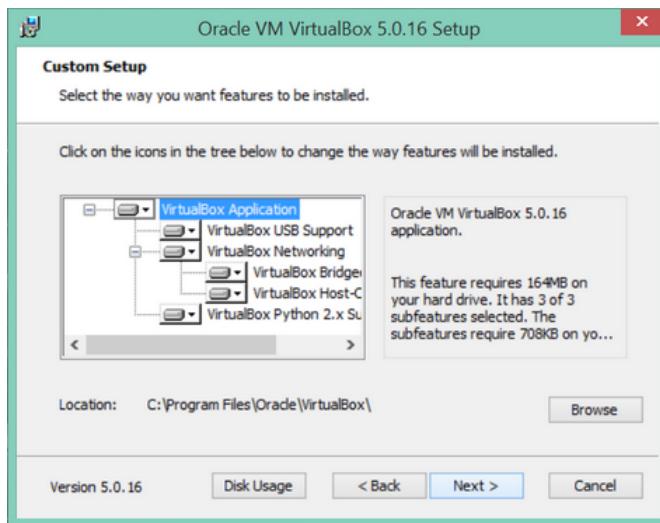
Em seguida escolha o download para **Windows** como na imagem abaixo.



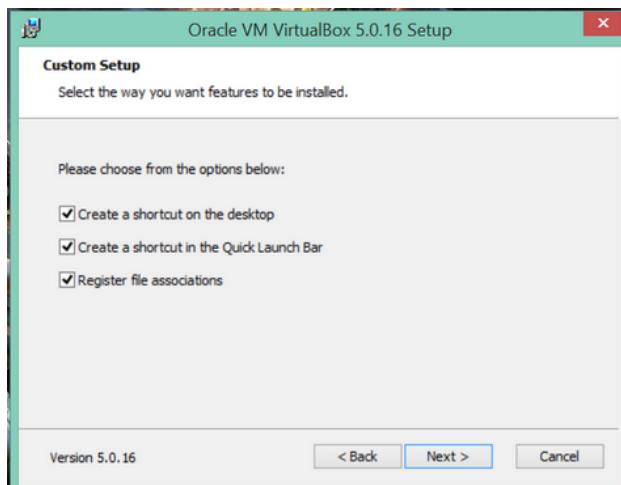
Após realizar o download vamos executar o executável que acabamos de fazer download, após clicamos em **next** como na imagem abaixo.



Agora realizamos algumas modificações na instalação, como iremos fazer uma instalação padrão vamos clicar em **next** igual a imagem abaixo.



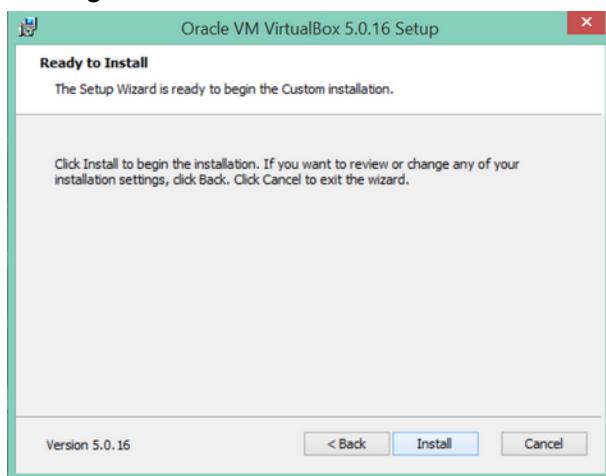
Novamente iremos clicar em **next**.



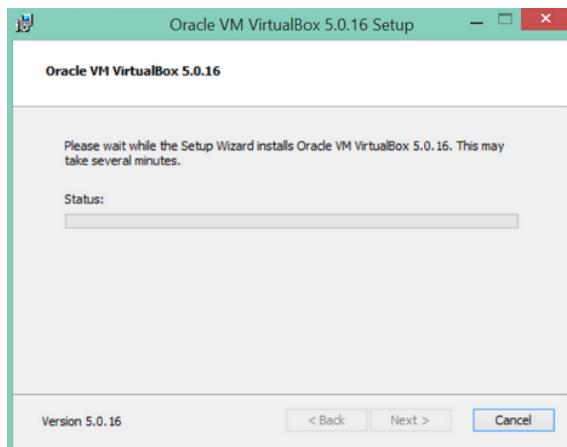
Em seguida clicamos em **yes** como na imagem abaixo.



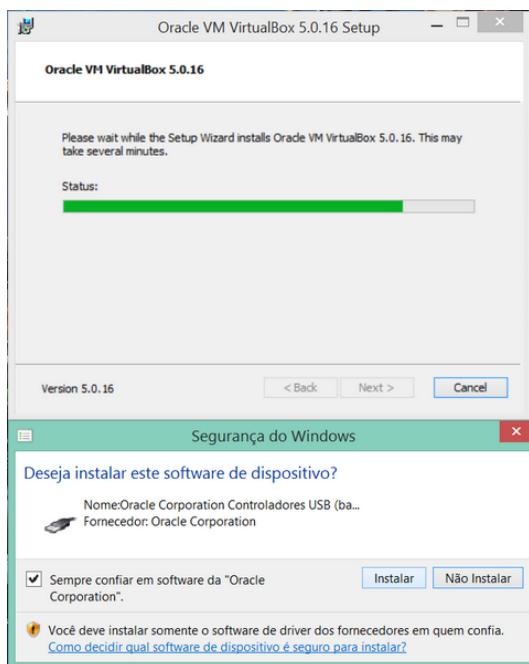
Em seguida **Install**.



Pode demorar um pouco a instalação dependendo do processamento do seu computador.



Durante a instalação será pedido permissão para instalar extensões. Clique em Instalar.



Como na imagem abaixo você pode escolher **Start** e já iniciar a máquina ou desmarcar e não iniciar agora. Após click em **finish**.



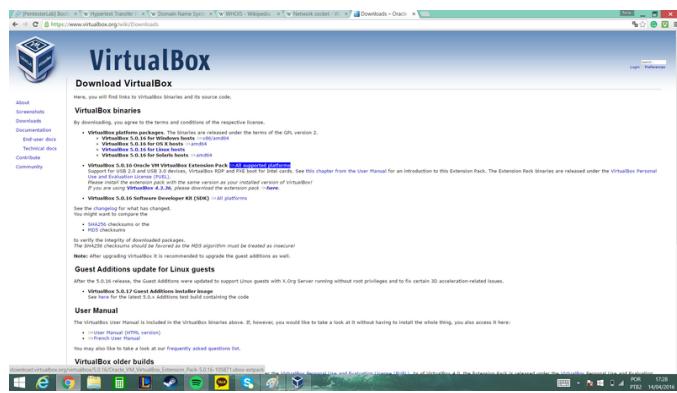
Depois de instalado e iniciado o virtualBox fica dessa forma.



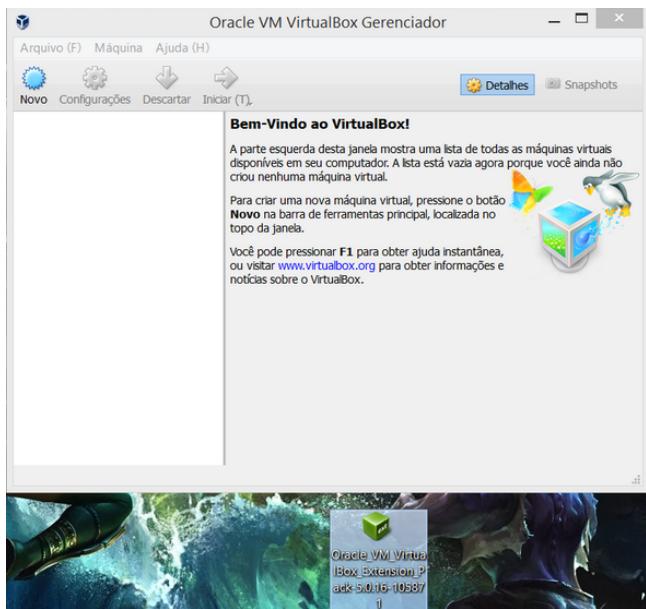
## 7.7 Instalando Extension Pack

Agora vamos instalar a **Extension pack**, para isso vá para a página de download do VirtualBox novamente como na imagem abaixo. Podemos realizar o download do extension pack no link abaixo.

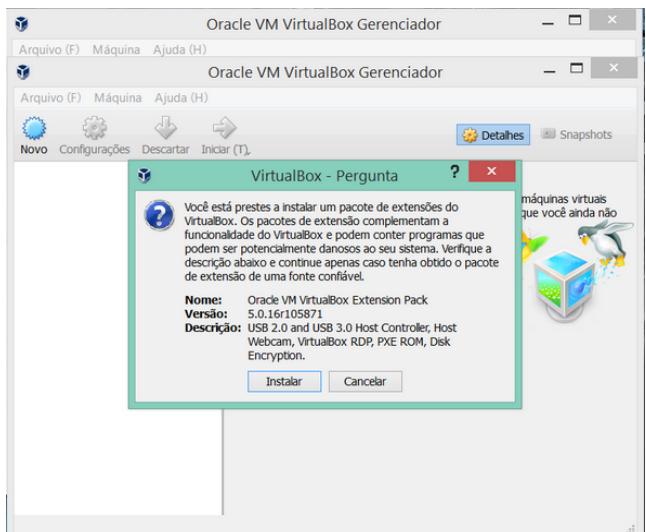
- <https://www.virtualbox.org/wiki/Downloads>



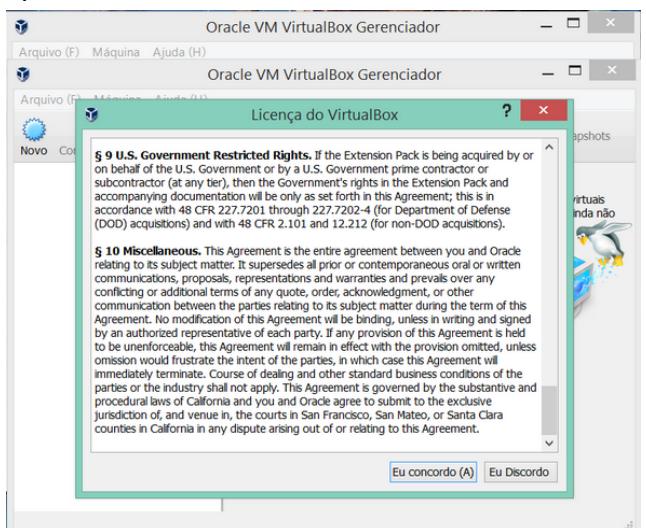
Feito o download é só executar a extensão que é multiplataforma.



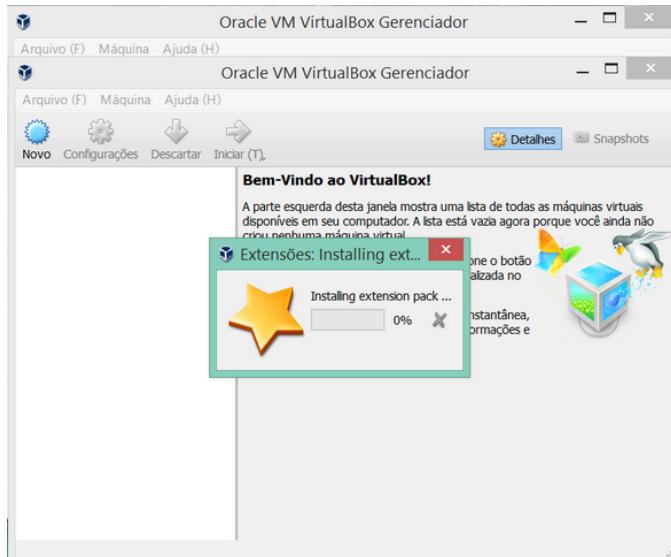
Em seguida clique em **instalar** como na imagem abaixo.



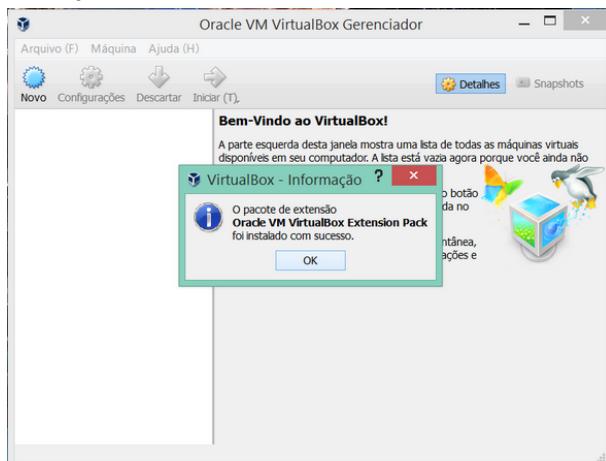
Após clicar em **instalar** aceite o contrato **Eu Concordo** com a próxima imagem.



Após clicar em aceito ele vai ser instalado.



Após já vai estar tudo OK.



Não esqueça de usar o extension pack na mesma versão do virtualbox.

## 7.8 Conhecendo o Genymotion Android

### 7.8.1 O que é o Genymotion?

O Genymotion é um projeto que tem como objetivo a emulação gratuita de sistemas operacionais Android.

Como ele podemos usar diversas versões, os respectivos aplicativos disponíveis e usar de forma virtualizada sem a necessidade de ter diversos dispositivos físicos.

### 6.8.2 Como ele pode nos ajudar ?

Com o Genymotion podemos realizar diversas ações, por exemplo:

- Emular um dispositivo Android;
- Obter root no dispositivo;

- Realizar download do APK.

Neste laboratório iremos:

- Criar o dispositivo Android para o laboratório;

### 6.8.3 Criando conta

#### 1. Criação de Conta:

- <https://www-v1.genymotion.com/account/create/>

The screenshot shows the Genymotion account creation interface. At the top, there's a navigation bar with links for 'Use Cases', 'Pricing', 'Integrations', 'Resources', and 'Company'. On the right side of the header is a 'Sign In' button. Below the header, a progress bar indicates the user is at Step 1 of 3. The main section is titled 'Register'. It contains several input fields: 'Email address\*' with a value 'gqvfaucxsmirvtdu@pp7rvv.com', 'Usage type\*' with a value 'Demonstration', 'Password\*' with a masked value, 'Company type\*' with a value 'Others', and a 'Country' dropdown set to 'Brazil'. At the bottom of the form, there are two checkboxes: one for accepting the 'privacy policy' and another for accepting 'the Terms and Conditions'. There are also checkboxes for 'I want the latest news and updates'. A large red 'CREATE ACCOUNT' button is positioned at the bottom right of the form area.

- Vou usar um email temporário: <https://10minutemail.com/>

### 6.8.4 Instalando Genymotion - Linux

O Genymotion tem como pré-requisito a instalação do VirtualBox previamente, dependendo da versão for realizado o download o mesmo já no instalador.

#### 6.8.4.1 Realizando download

No link abaixo podemos realizar o download do genymotion:

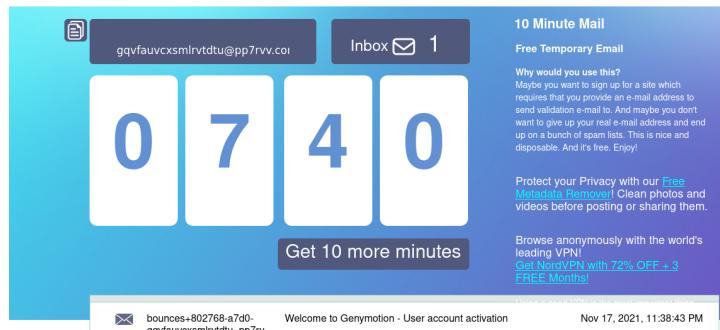
- <https://genymotion.com/download>

The screenshot shows the Genymotion download page. At the top, there are navigation links: Genymotion, Use Cases, Pricing, Integrations, Resources (selected), and Company. Below the header, a main title says "Download Genymotion Desktop 3.2.1". There are two main sections for Linux and macOS, each with its own system requirements and download links. Under the Linux section, there are two options: "Ubuntu 20.04 LTS, Debian 9+, Fedora 30+ (64bit)" and "Ubuntu 20.04 LTS Focal Fossa - 64bit only". Both have "Download for Linux (48MB)" and "Checksum (SHA-1)" links. The first section also has a "Get started" button. The macOS section has "macOS 10.13 (High Sierra), 10.14 (Mojave), 10.15 (Catalina) or 11(Big Sur)" and "Download for macOS (44MB)" with "Checksum (SHA-1)". Below these are sections for Windows, including "without VirtualBox" (Windows 8.1, 10, Intel VT-x/AMD-V/SVM, 4GB RAM, 400 MB disk space, VirtualBox 6.1.16) and "with VirtualBox" (Windows 8.1, 10, 41MB, VirtualBox 6.1.16). Each has a "Download for Windows" link and a "Checksum (SHA-1)" link.

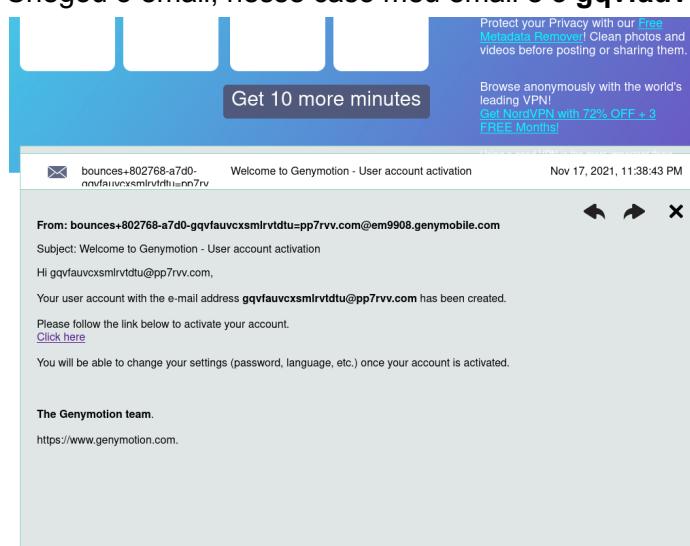
## 6.8.4.2 Documentação

### Documentação

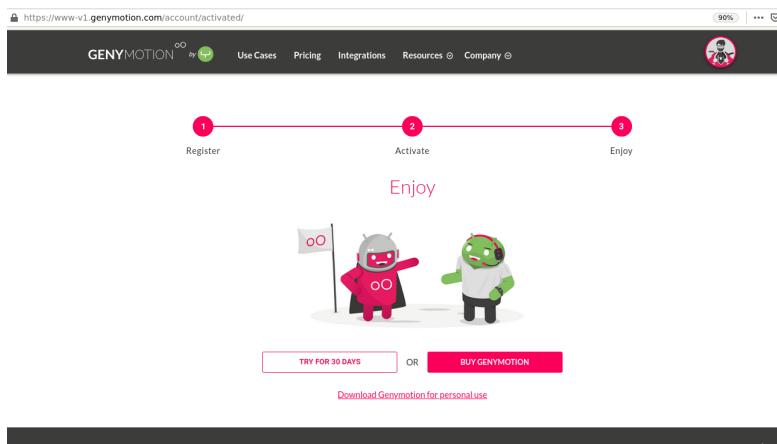
- <https://docs.genymotion.com/desktop/latest/>



Chegou o email, nesse caso meu email é o **gqvfauvcxsmirvtdu@pp7rvv.com**.



Agora vamos escolher qual versão usar, vou usar gratuita por 30 dias e que tem o nome de **TRY FOR 30 DAYS**.



#### 6.8.4.3 Observações

Podemos usar online e pagamos por hora Android e IOS.

- IOS só na nuvem

É recomendado o uso de um dispositivo físico devido a estabilidade, velocidade e minimizar possíveis problemas.

#### 6.8.4.4 Comandos para instalação

Para dar a início a instalação:

```
cd /tmp
wget -c
https://dl.genymotion.com/releases/genymotion-3.2.1/genymotion-3.2.1-lin
ux_x64.bin
chmod +x genymotion-3.2.1-linux_x64.bin
sudo ./genymotion-3.2.1-linux_x64.bin
```

Vamos criar um script com as informações acima e dar o nome de **install\_genymotion.sh**.

```
greenmind@job:~$ cat install_genymotion.sh
cd /tmp
wget -c https://dl.genymotion.com/releases/genymotion-3.2.1/genymotion-3.2.1-linux_x64.bin
chmod +x genymotion-3.2.1-linux_x64.bin
sudo ./genymotion-3.2.1-linux_x64.bin
```

Vamos dar permissão de execução usando **chmod**.

```
chmod +x install_genymotion.sh
```

Podemos ver o resultado.

```

greenmind@ub:~$ sudo ./install_genymotion.sh
2021-11-17 20:47:17 - https://dl.genymotion.com/releases/genymotion/3.2.1/genymotion-3.2.1-linux_x64.bin
Resolvendo o download de https://dl.genymotion.com... 104.18.111.50, 104.17.171.23, 2606:4700::6811:a017, ...
Conectando-se a dl.genymotion.com (dl.genymotion.com)[104.18.111.50]:443... conectado.
A requisição HTTP foi enviada, aguardando resposta... 200 OK
Tamanho: 48264053 (46M) [application/octet-stream]
Salvando em: "genymotion-3.2.1-linux_x64.bin"

genymotion-3.2.1-linux_x64.bin          100%[=====] 46,03M 10,4MB/s   em 4,6s
2021-11-17 20:47:21 (10,1 MB/s) - "genymotion-3.2.1-linux_x64.bin" salvo [48264053/48264053]

Installing for all users.

Installing to folder [/opt/genymobile/genymotion]. Are you sure [y/n] ? y

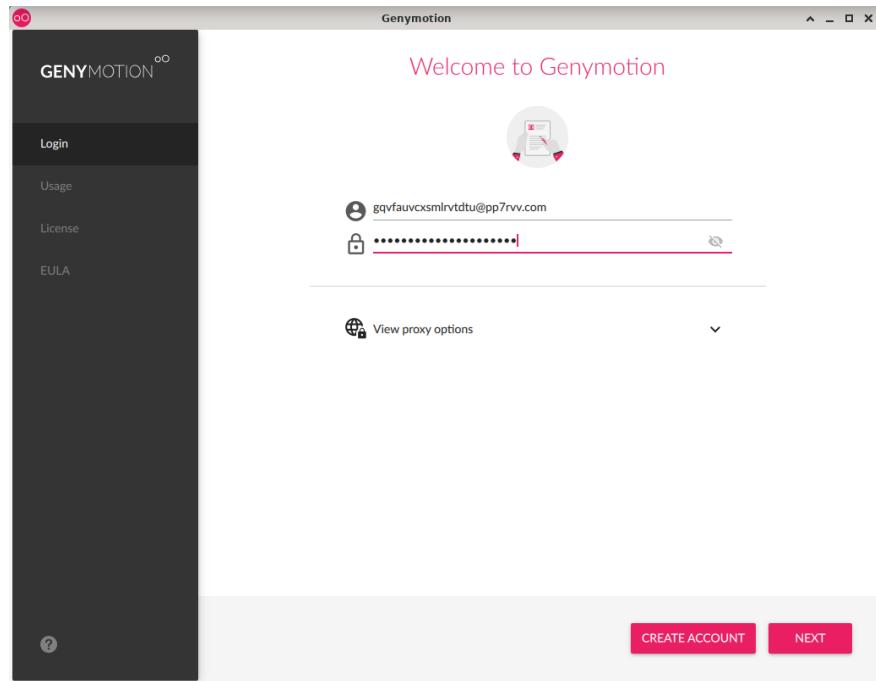
- Trying to find VirtualBox toolset ..... OK (Valid version of VirtualBox found: 6.1.28r147628)
- Extracting files ..... OK (Extract into: [/opt/genymobile/genymotion])
- Installing launcher icon ..... OK

Installation done successfully.

You can now use these tools from [/opt/genymobile/genymotion]:
- genymotion
- genymotion-shell
- gmttool

```

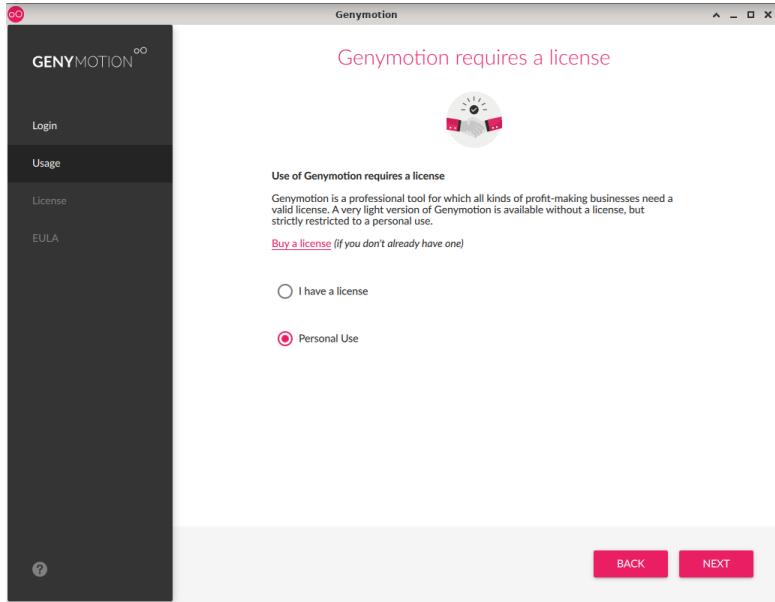
Vamos realizar o login na conta.



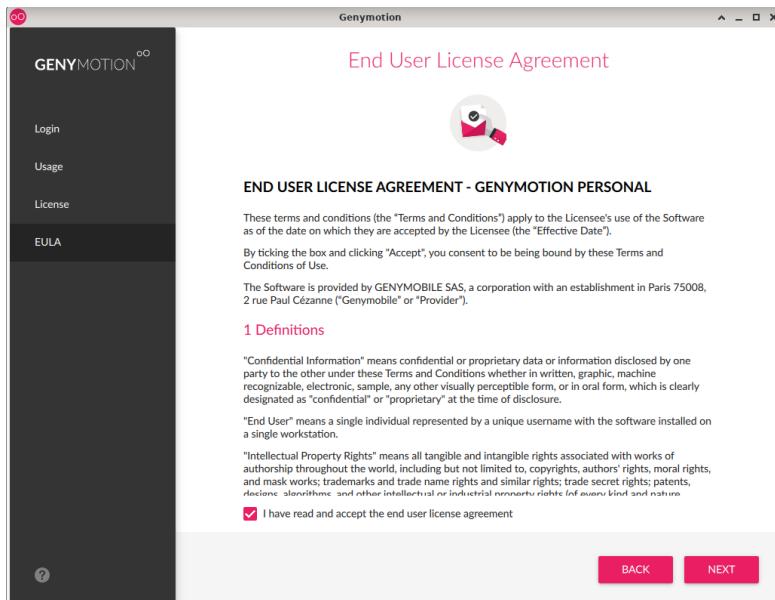
Caso não tenha feito conta pode ir até **CREATE ACCOUNT**. Vamos ser redirecionados.

- <https://www-v1.genymotion.com/account/create/>

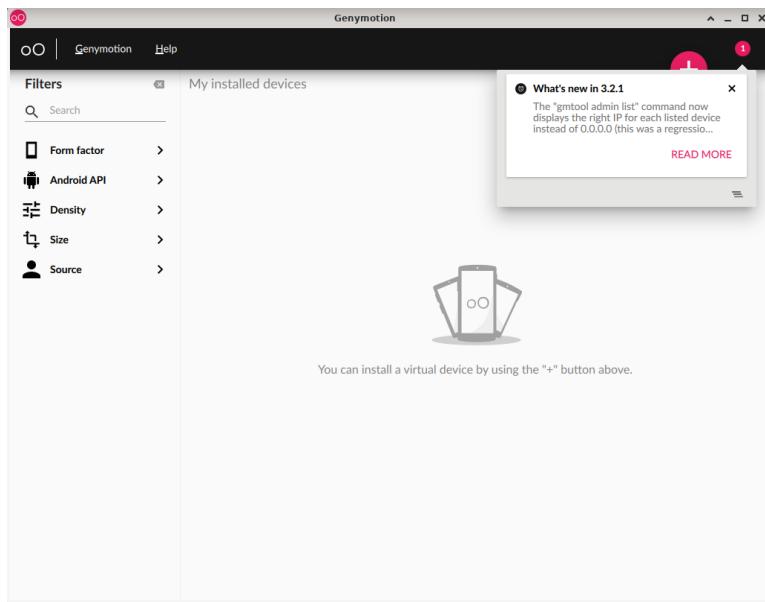
Vamos setar **Personal Use**.



Vamos aceitar a licença.



Essa é a página principal.



## 6.8.5 Instalando Genymotion - Windows

### 6.8.5.1 Realizando download

No link abaixo iremos realizar o download do Gentmotion.:

- <https://genymotion.com/download>

Vamos usar a versão Windows e temos 2 opções:

- A primeira opção é com o Virtualbox;
- A Segunda opção é sem o Virtualbox(que possivelmente será instalado junto com o genymotion);

### 6.8.5.2 Iniciando instalação

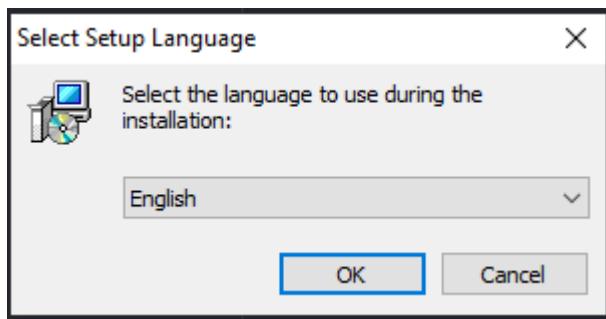
### 6.8.5.3 Permissão de administrador

Vamos conceder permissão de execução ao instalador.

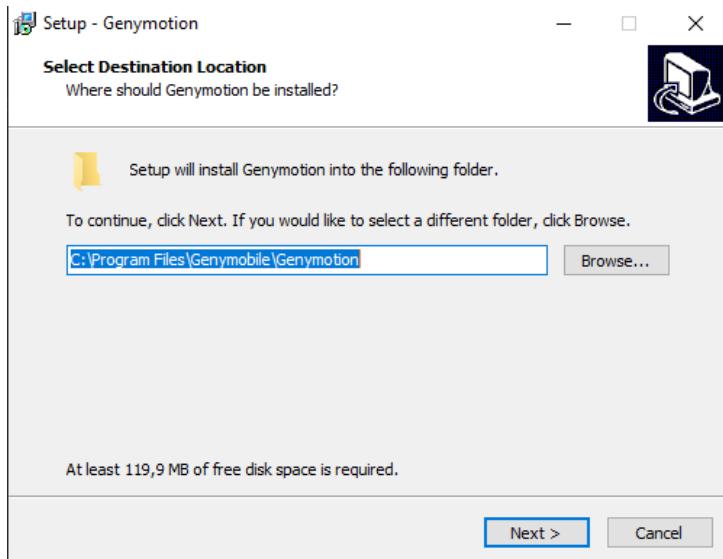
### 6.8.5.4 Escolher a língua de Instalação

Temos duas que são:

- Inglês;
- Francês;



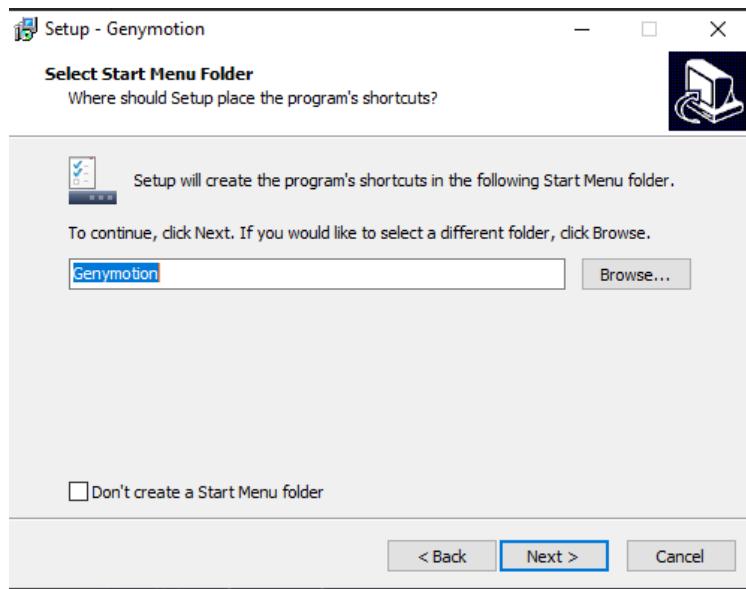
#### 6.8.5.5 Localização



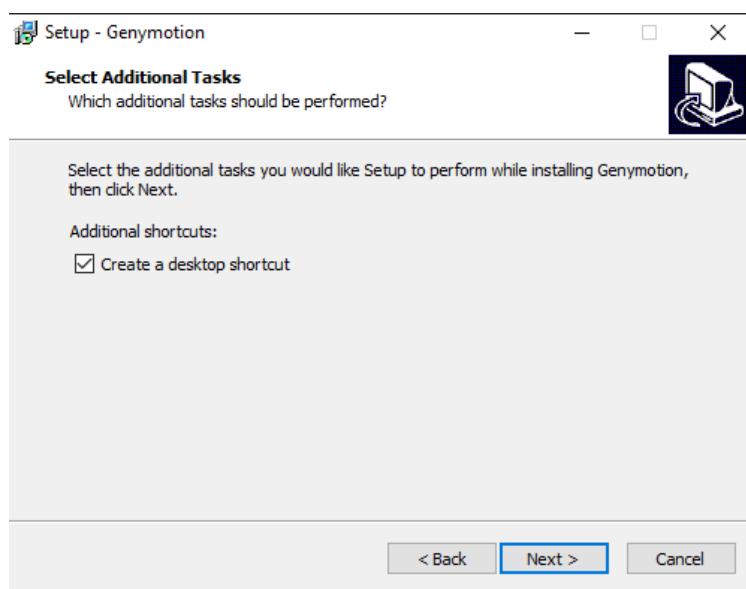
Vamos escolher a localização para a instalação.

#### 6.8.5.6 Nome menu principal

Vamos escolher o nome do link no menu principal.

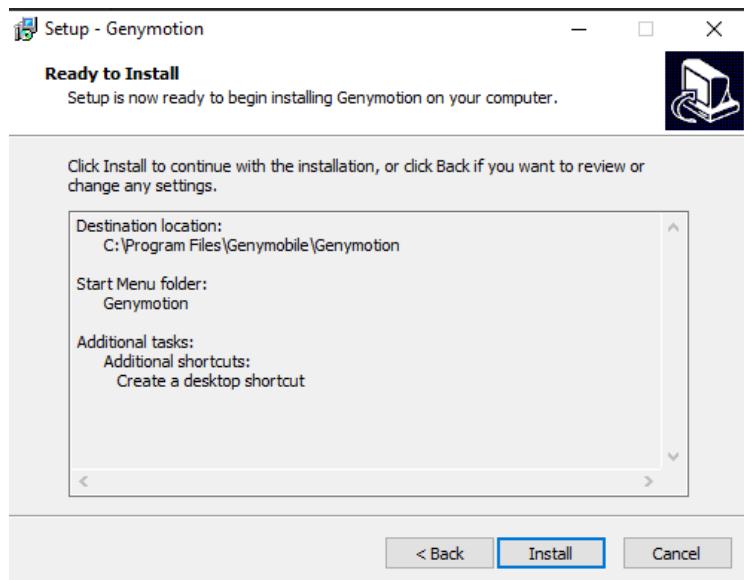


#### 6.8.5.7 Shortcut

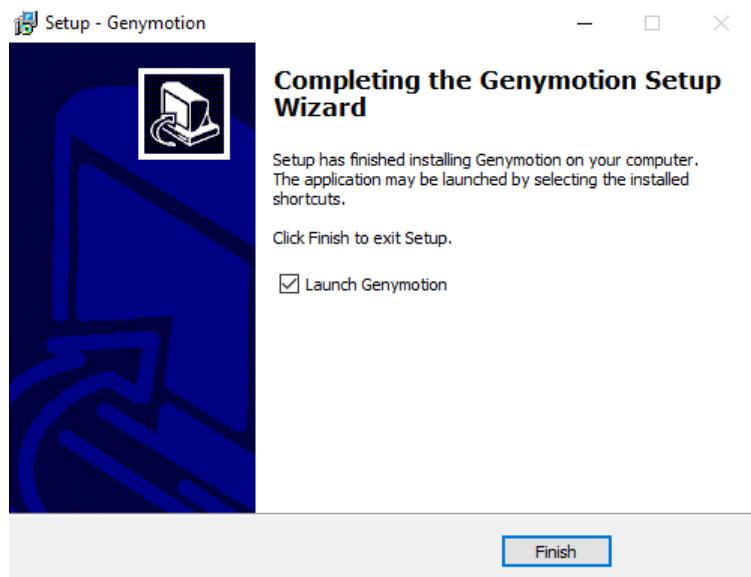


#### 6.8.5.8 Instalando

Iniciar a instalação.



Finalizando instalação.



## 6.9 Criando máquina Kali Oficial - Virtualbox

### 6.9.1 Criando máquina Kali Oficial - Virtualbox

#### 6.9.2 O que é o Kali Linux

O Kali Linux que antigamente era conhecido como BackTrack Linux é uma distribuição Linux que é baseada em Debian e tem o código aberto voltada para testes de penetração avançados e auditoria de segurança.

O Kali Linux contém diversas de ferramentas voltadas para diversas tarefas de segurança da informação, como pentesters, computação forense e engenharia reversa.

Kali Linux foi lançado em 13 de março de 2013 como uma reconstrução completa de cima para baixo do BackTrack Linux, aderindo completamente aos padrões de desenvolvimento do Debian.

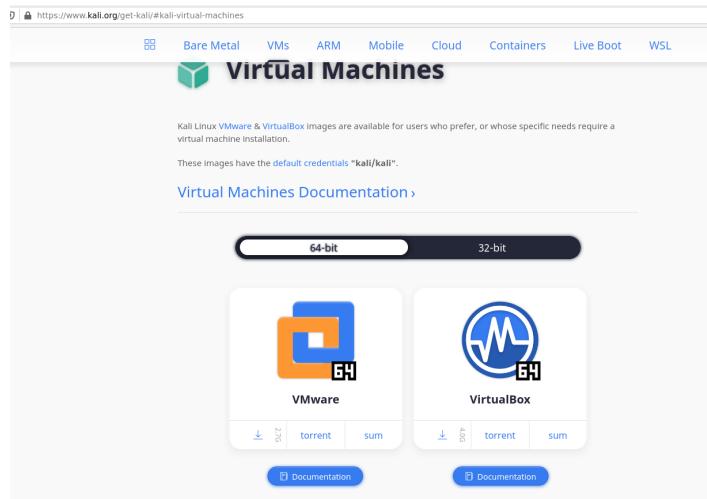
- <https://www.kali.org/docs/introduction/what-is-kali-linux/>

### 6.9.3 Site oficial

- <https://www.kali.org/>

### 6.9.4 Download

- <https://www.kali.org/get-kali/#kali-virtual-machines>



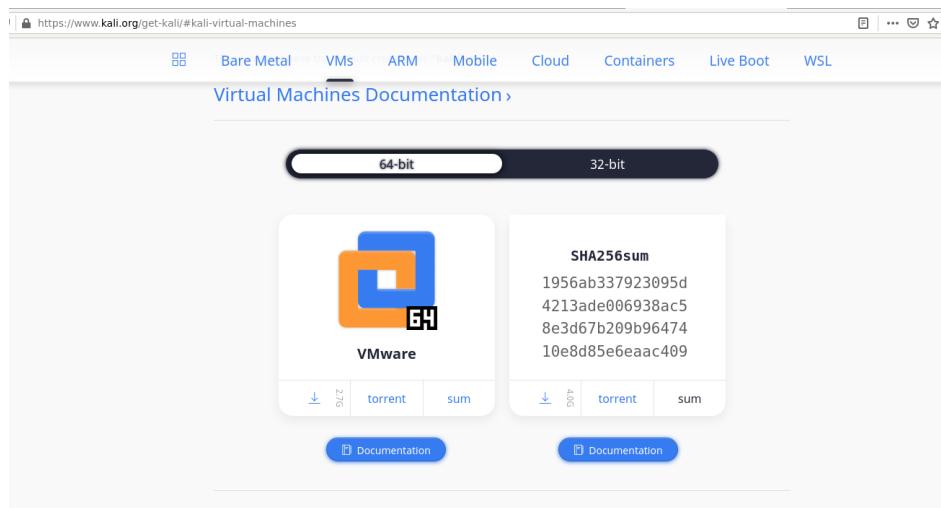
Como estamos realizando o uso do Virtualbox, vamos realizar o download da máquina virtual para o Virtualbox.

Podemos usar o link abaixo para realizar o download:

- <https://kali.download/virtual-images/kali-2021.3/kali-linux-2021.3-virtualbox-amd64.ova>

DICA: Recomendo **uGet** para gerenciar o download e assim ser mais rápido o download da imagem.

Vamos checar se a imagem está tudo **ok** e confirmar que a imagem não está corrompida ou foi modificada.



- SHA256sum:  
1956ab337923095d4213ade006938ac58e3d67b209b9647410e8d85e6eaac409

## 6.9.5 Verificando ISO

Vimos anteriormente que tínhamos uma **SHA256sum** ao realizar download do kali, agora vamos checar a ISO:

```
sha256sum kali-linux-2021.3-virtualbox-amd64.ova
```

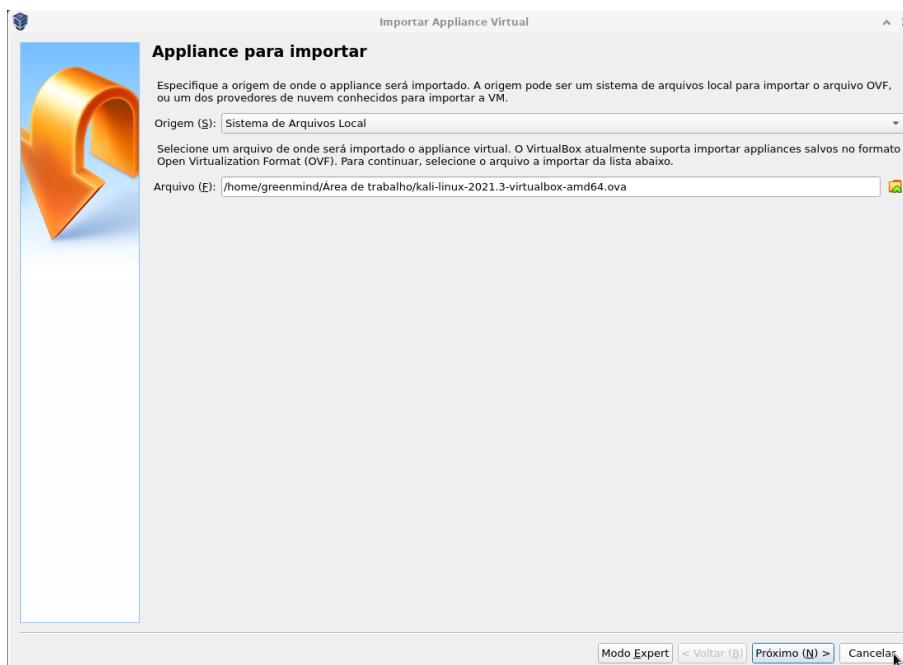
## 6.9.6 Importando máquina

Vamos agora importar nossa máquina para o nosso Virtualbox.

Vamos abrir o virtualbox.



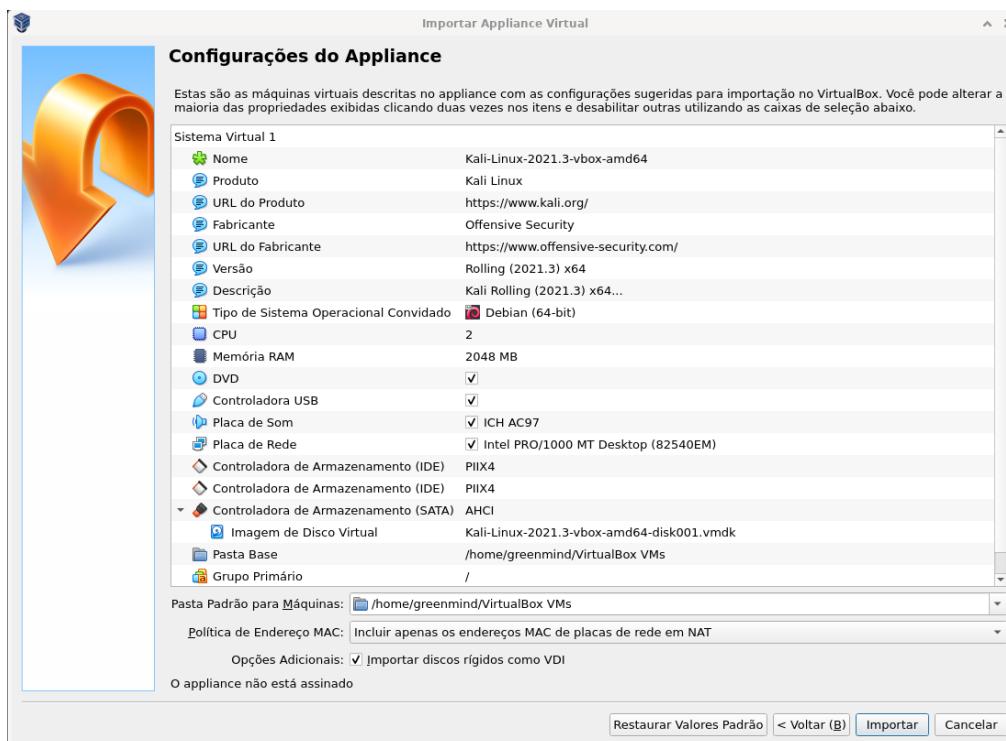
Vamos clicar em **Importar** para realizar a importação da máquina.



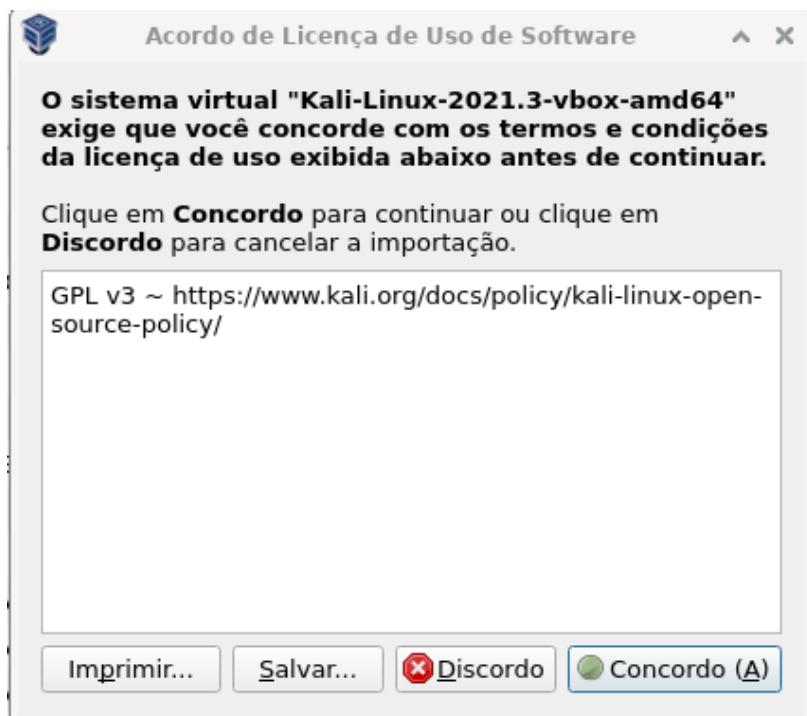
- Em seguida, vamos clicar em **Próximo**.

Agora podemos ver informações da nossa máquina como memória utilizada, CPU, placa de rede usada e etc.

- Vamos finalizar clicar em **Importar**.



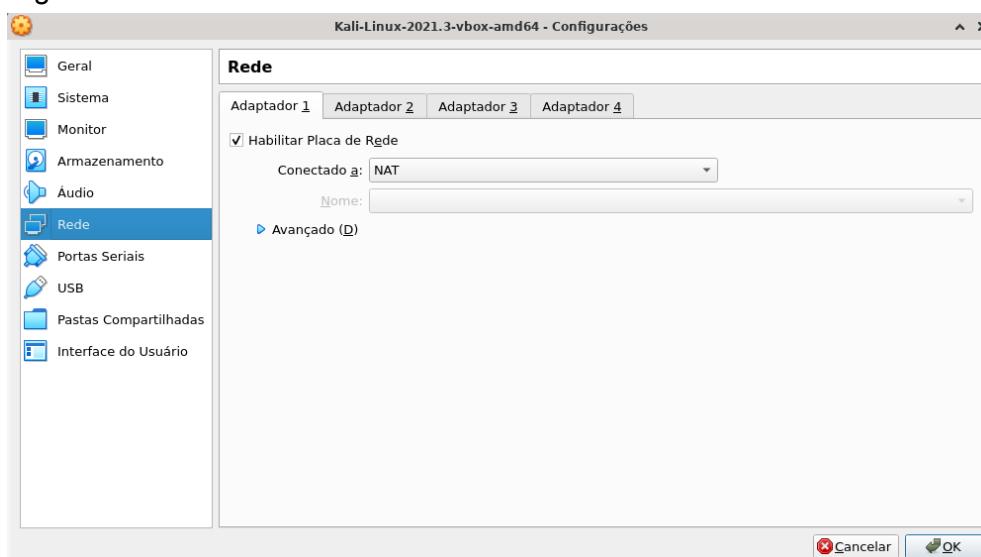
Vamos aceitar os termos e condições do Kali.



- **Concordo (A)**

### 6.9.7 Configurando - Rede

Podemos configurar nossa rede de forma simples, basta clicarmos em **configurações** e em seguida em **rede**.



Em seguida, só precisamos clicar em **OK**.

### 6.9.8 Alterando usuário

Por padrão a máquina vem com o usuário e senha:

- kali
- kali

Recomendo alterar usando usando o passwd:

```
passwd
```

O mesmo para o usuário **root**.

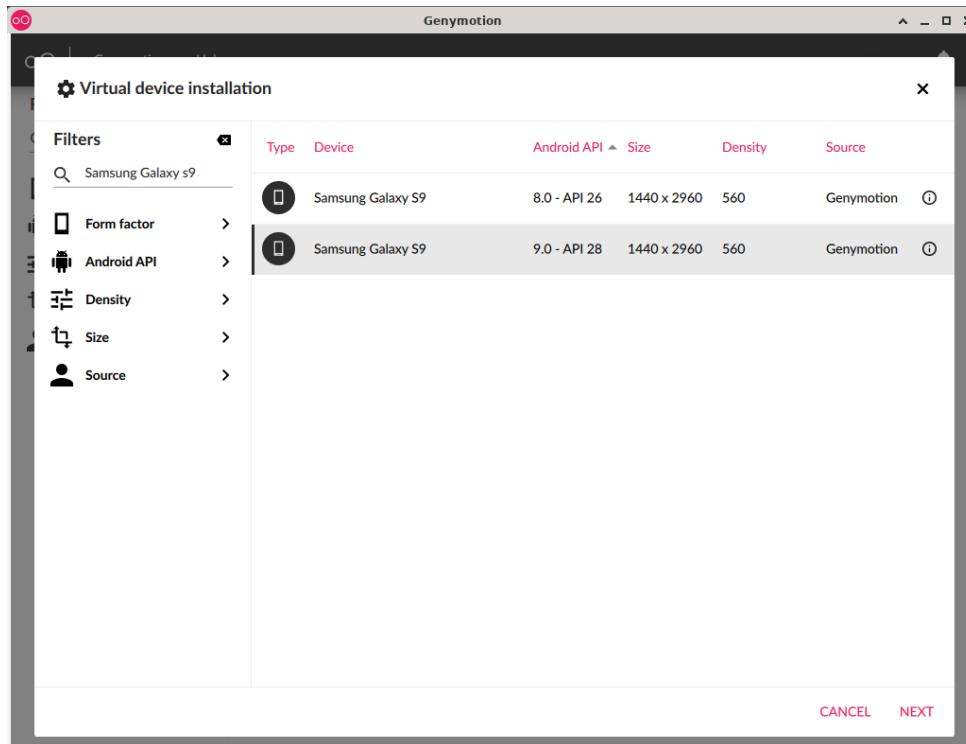
```
sudo su  
passwd
```

DICA: Não esqueça a senha

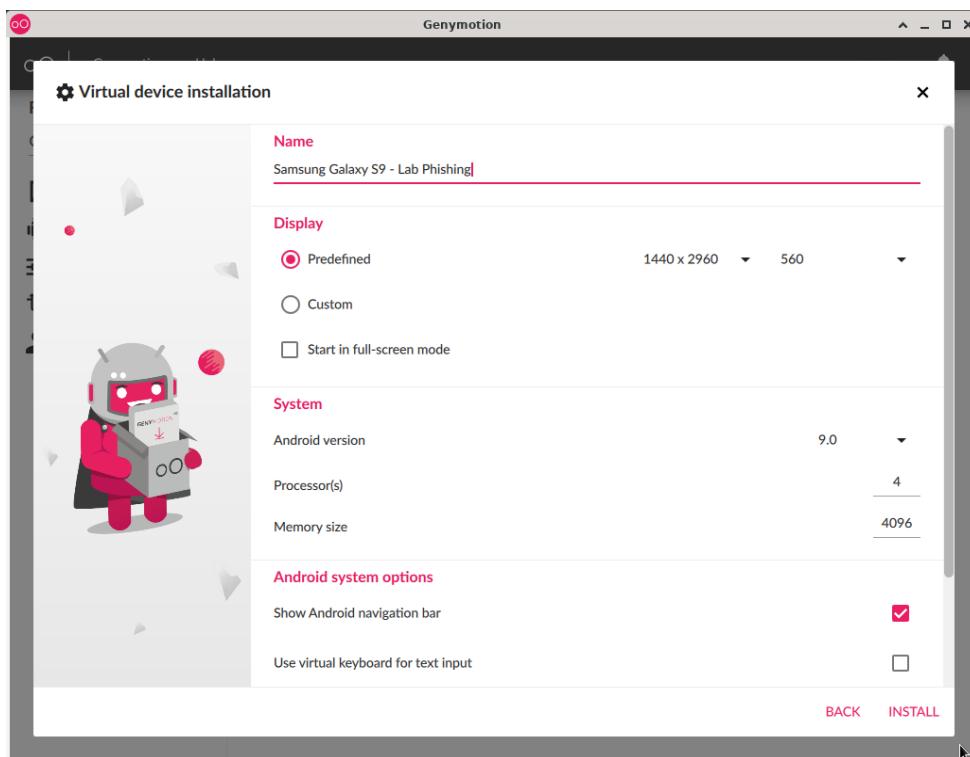
## 6.10 Criando laboratório Android - Genymotion

### 6.10.1 Criando laboratório Android - Genymotion

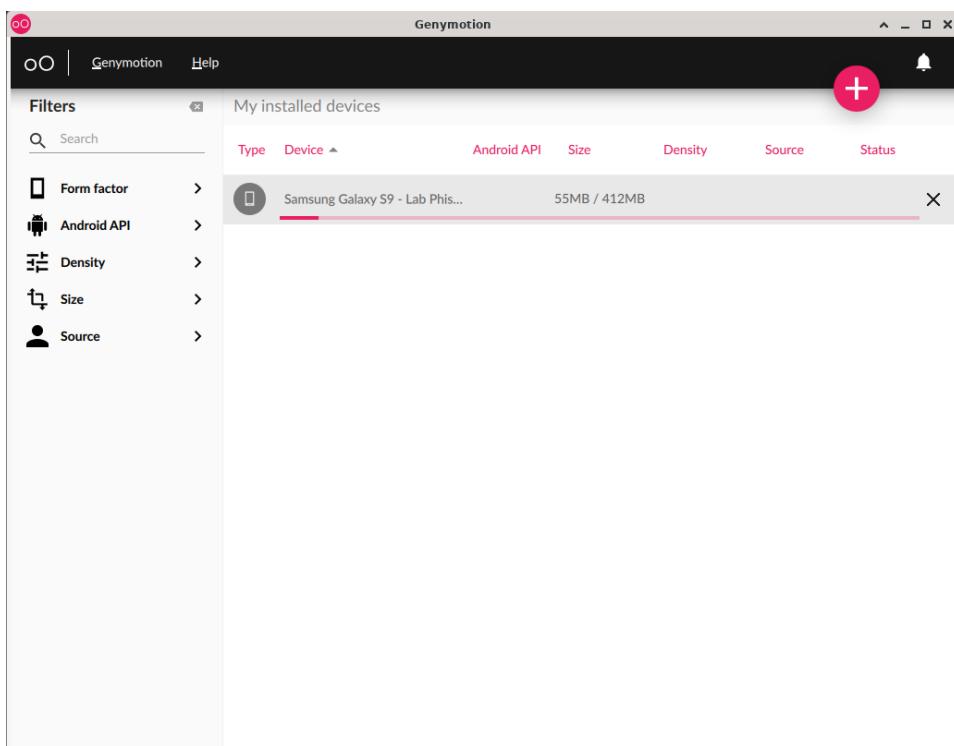
Vamos clicar no **+**, vamos setar o valor **Samsung Galaxy s9**. Vamos selecionar o **Samsung Galaxy** da sua escolha, em seguida vamos clicar em **Next**.



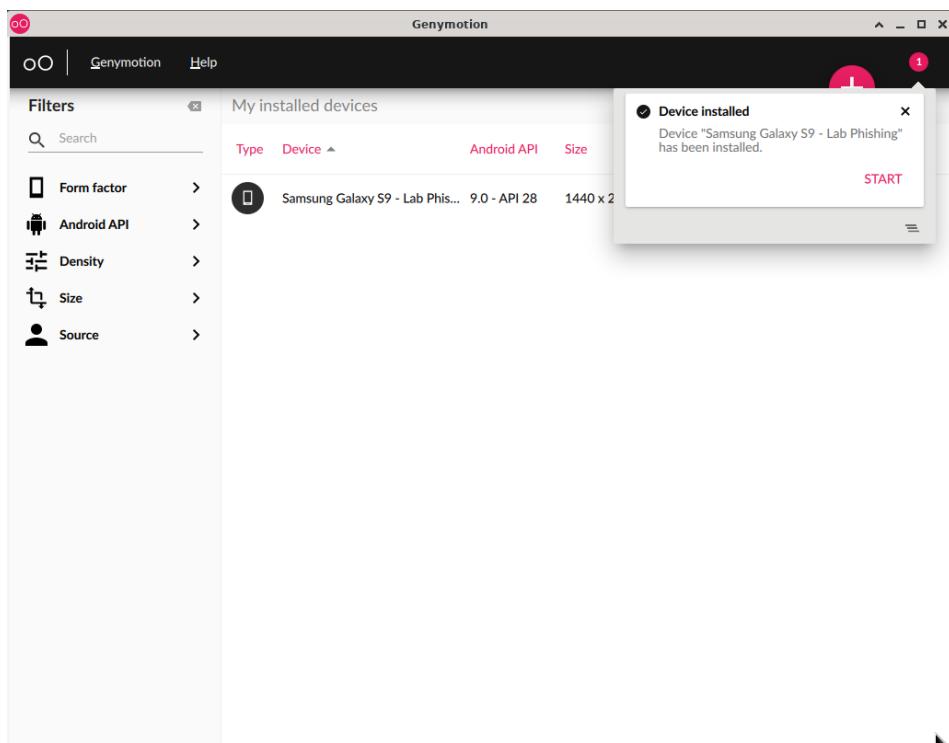
Agora vamos dar um nome para esse ambiente e clicar em **Install**.



Download está sendo realizado.



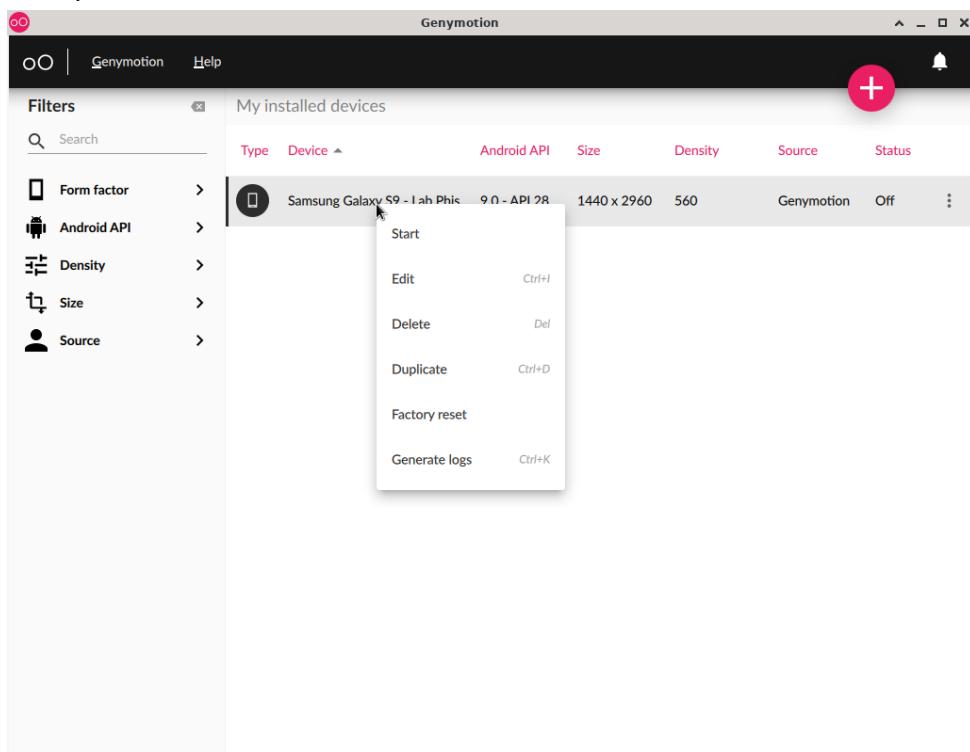
Após será realizado a criação do laboratório.



DICA: É recomendado que seja alterado para o local.

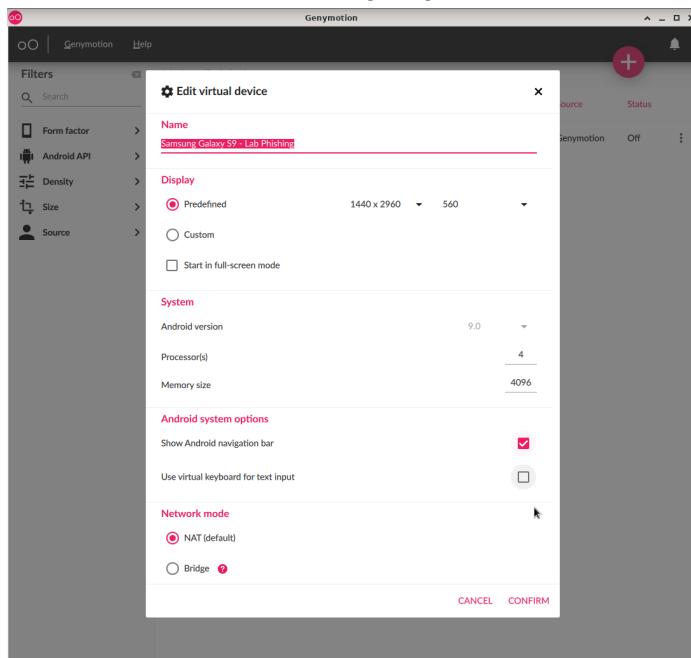
```
/opt/genymobile/genymotion/tools
```

Iniciando a máquina podemos clicar com o botão direito em cima da máquina e clicar em **start** para iniciar.

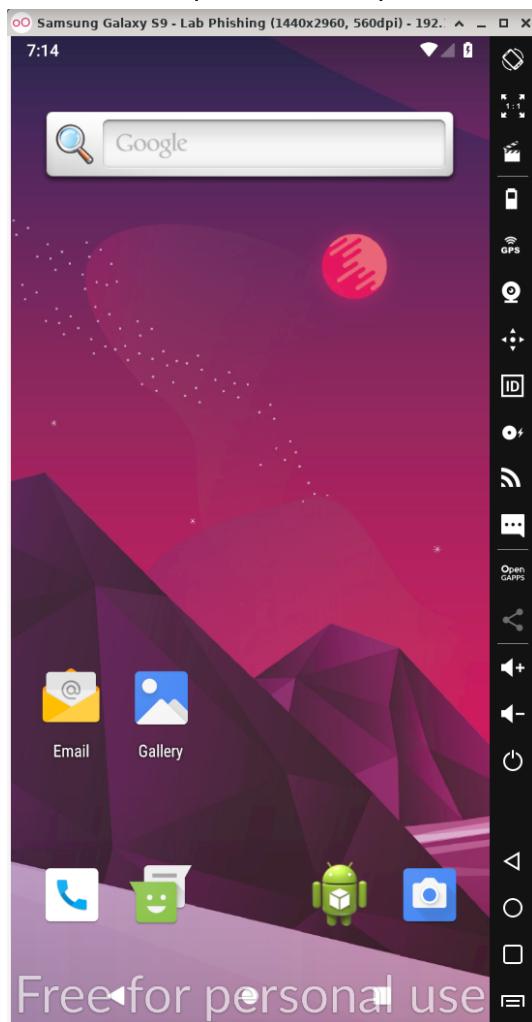


Caso tenha algum problema ou já tenha usado a máquina clique em **Reset Factory**.

A máquina vem com a configuração de rede **NAT** por padrão.



Podemos ver que nossa máquina com Android foi criada.



## 8. Criando lista de visibilidade

### Criando nossa lista de visibilidade

Podemos levantar com os times da empresa todas informações que desejam monitorar, sejam domínios oficiais, campanhas de marketing, redes sociais e diversas informações que pessoas má intencionadas possam ter a fim de monitorar.

### O que é lista de ativos ou lista de visibilidade ?

Lista de ativos, lista de visibilidade e até outros nomes, é um documento que armazena todas as informações verdadeiras que desejam monitorar, sejam elas imagens de logo, imagem da marca da empresa, urls das redes sociais oficiais, domínios oficiais, IPS, blocos de IPS, aplicativos oficiais e até palavras chaves que podem ser usadas por serviços.

### Como podemos nos beneficiar?

Com essas informações armazenadas conseguimos nos guiar melhor durante as buscas para capturar informações, além disso empresas parceiras podem ser beneficiadas com essas informações e outras antes mesmo de começar precisar dessa lista em mãos para iniciar as buscas.

Precisamos conversar com outros times da mesma empresa como o time de infraestrutura ou até o red team, além disso empresas parceiras e até coligadas. Documentar todos os endpoints, urls usadas e manter atualizada pode ajudar no monitoramento. Não serão apenas esses times que serão beneficiados, todos os times que precisam dessas informações podem usar como por exemplo o time de análise de vulnerabilidades.

As consultorias muitas vezes não conhecem como funciona a empresa, quais são os IPS, domínios, aplicativos e com essa lista ela consegue ter a visão do que precisa buscar na internet. Dessa forma as buscas são mais assertivas e retornando resultados melhores.

### Quais informações são importantes ?

Abaixo irei explicar algumas informações que não podem faltar.

#### Logo e imagens de produtos

As logos ou até imagens de projetos e produtos podem ser usadas para a busca de informações, conseguimos realizar uma busca reversa de imagens e assim conseguindo ter visibilidade de outros sites que estão usando essa imagem.

Podemos ver abaixo dois projetos que podem nos ajudar com isso e são:

- Google Imagens - <https://images.google.com>
- Tineye - <https://tineye.com>

## URLs (redes sociais)

Devido ao aumento de páginas falsas o monitoramento das redes sociais ficou indispensável, estamos acompanhando o grande aumento de páginas ou até o roubo de páginas com muita visibilidade. O monitoramento de páginas nas redes sociais são essenciais para evitar que seus clientes ou até funcionários sejam fiscados pelos atacantes.

Para isso devemos sempre levantar todas as páginas oficiais e enviar para o time. Caso encontre alguma página suspeita, relate ou até peça o takedown dessa informação. Empresas que lidam com o público e prestam serviços financeiros podem ter um impacto maior já que o prejuízo financeiro é muito grande.

Levante as redes sociais:

- Facebook
- Instagram
- Youtube
- Twitter
- Entre outras(dependendo no nicho de negócio)

Caso possua grupos em aplicativos de mensagem, deixe salvo e busque por grupos suspeitos.

## Domínios

Os domínios são a nossa "identidade na internet", muitas vezes é o primeiro contato devido aos motores de busca e cuidar dos nossos domínios é um item crítico. Atualmente devido a falta de documentação ou até a atualização do documento muitos domínios não são monitorados e isso pode ser um risco reputacional ou aos envolvidos.

Como vimos anteriormente podemos ver como criminosos podem encontrar sites semelhantes para as suas campanhas de phishing, dessa forma precisamos ficar de olho. Além disso, muitos criminosos utilizam propagandas patrocinadas usando soluções pagas para deixar suas campanhas no topo. Algumas soluções que podem ser usadas:

- Google AdSense
- Google Ads

Para piorar o cenário muitas empresas acabam criando diversos domínios, dessa forma funcionários e clientes podem se confundir quais são os verdadeiros e os falsos. Dessa forma, recomendo centralizar os serviços em domínios conhecidos usando subdomínios ou até subdiretórios. Evite criar um domínio apenas para o RH por exemplo. Sites gerenciais tomem cuidado com a exposição com a internet, recomendo o uso de VPN é só deixar expostos para a internet o que for realmente necessário.

Depois de saber tudo isso vamos levantar todos os nossos domínios oficiais, os domínios de coligadas e de prestadores de serviço. Dessa forma iremos conseguir ter a visibilidade do que está exposto ou não.

## IPS ou blocos de IPS

Além dos domínios expostos na internet a monitoração de exposição de IPS é muito importante, esse tipo de trabalho é essencial para uma maior segurança ou até evitar o acesso indevido a sistemas internos.

Conseguimos buscar por informações usando o nome da empresa que está no CNPJ, as palavras chaves usadas na rede podem nos auxiliar na busca por informações. Usando o Shodan por exemplo conseguimos filtrar por cidade e assim encontrando possíveis IPS expostos de uma determinada empresa.

Quando estamos em uma empresa grande, muitas vezes ela compra uma grande quantidade de IPS ou até blocos de IPS, monitorar os IPS e o quanto exposto eles estão é muito válido. Além disso, catalogue também os IPS de coligadas e IPS de prestadores de serviço e assim ajude seu time ou consultores a ter uma maior visibilidade da exposição na internet.

## Aplicativos oficiais

O aumento do uso dos aplicativos não é novidade, muitas pessoas estão usando cada vez mais celulares, sejam os jovens e até os idosos. Devido a facilidade para a instalação de um aplicativo e a grande quantidade de documentações para a criação de aplicativos o aumento de aplicativos suspeitos vem aumentando.

Antigamente o perigo era só as **Lojas oficiais**, mas com o tempo outras **Lojas não oficiais** surgiram trazendo com elas uma leva de aplicativos maliciosos. Muitas vezes usuários querem ter acesso a uma versão antiga que funciona no seu celular, outros buscando por aplicativos pagos em lojas não oficiais de forma gratuita. Junto com eles vem os **Malwares** e os **Roubos de informações**.

Devido a isso é muito importante o levantamento dos aplicativos oficiais, sejam nas lojas:

- Apple Store
- Google Play

Qualquer outra podemos levantar como suspeitos em muitos casos.

Dessa forma outros times podem ter a visibilidade do que é oficial e o que pode ser pedido para ser retirado da internet.

- Por exemplo, a quantidade de aplicativos suspeitos do **auxílio emergencial** é muito maior que os oficiais do próprio governo.

## Palavras chaves

As palavras chaves nos auxiliam a uma melhor busca, dessa forma conseguimos ser mais assertivos nas buscas ou até na criação de dorks. Mas essas palavras vai muito com o negócio em que você faz parte, por exemplo:

- Caso seja do setor financeiro as palavras chaves(aprovada, esquema e cartão são mais válidas do que vulnerabilidade, vazamento ou leak) para o time de fraudes.

No caso de páginas de phishings, muitas vezes essas páginas costumam ser semelhantes às páginas oficiais e assim muitas vezes ludibriam quem acessa. Claro que também podemos ver os phishings com o foco em usuários que buscam por prêmios ou benefícios,

As empresas também podem ser prejudicadas, devido aos funcionários receberem falsas mensagens de alertas ou avisos importantes com foco na captura de credenciais. Leve sempre a sua área de atuação e negócio em consideração na hora de criar as palavras chaves para a realização das buscas.

## Serviços

Use os serviços como palavras chaves, isso pode auxiliar na hora de sua busca e assim mirando em serviços específicos. Saiba quais são as palavras que se encaixam nesse contexto de serviços ou até técnicas usadas por criminosos para realizar uma dork(Busca avançada do Google).

Por exemplo:

- Cartão Crédito(Aprovada, burlando, conta, clonado);

Nomes internos(redes, siglas especiais)

Nomes internos podem ajudar a buscar por informações indexadas na internet, vazamento de informações em sites ou até páginas que simulam sua página verdadeira. Além disso, o excesso de exposição pode facilitar quando um atacante estiver em sua rede.

Busque levantar as seguintes informações:

- Siglas especiais;
- Nomes de rede;
- Padrões de emails;
- Projetos especiais;

## Criando nossa lista de palavras chaves

Busque levantar as seguintes informações:

- Qual o seu seguimento
- Quais as maiores fraudes acontecendo e que deseja buscar
- Girias usadas para o seu seguimento

## 9. TLDs

### O que é TLDs?

TLD, ou Top Level Domain, é a parte final de um endereço de um site que vem logo após o nome.

Por exemplo:

- badbank(nome do site)
- .com.br(TLD)

Para melhor entendimento, o TLD seria a exata localização de uma empresa, seu endereço completo. Por exemplo:

- badbank.com.br

Alguns exemplos de TLD são:

- .com
- .com.br
- .fun
- .info
- .com
- .us
- .co
- entre outros

Obviamente, ele não está em um domínio ao acaso, seu objetivo é realizar uma espécie de classificação do site. Ou seja, um site comercial cujo top-level domain é .com está informando que se trata de um site comercial.

Outro exemplo que temos é o WordPress.com, que é um site comercial, enquanto o WordPress.org se trata de uma versão sem fins lucrativos do grupo.

Podemos ver algumas lista de TLDs no site oficial da IANA

- Lista de TLDs da **IANA** - <https://data.iana.org/TLD/tlds-alpha-by-domain.txt>

```
# Version 2022090201, Last Updated Sat Sep 3 07:07:02 2022 UTC
AAA
AARP
ABARTH
ABB
ABBOTT
ABBVIE
ABC
ABLE
ABOGADO
ABUDHABI
AC
ACADEMY
ACCENTURE
ACCOUNTANT
ACCOUNTANTS
ACO
ACTOR
AD
ADAC
ADS
ADULT
AE
AEG
AERO
```

Ou uma lista completa disponível e as novidades que serão lançadas em TLDs.

- TLDs de A a Z - <https://tld-list.com/tlds-from-a-z>



a

---

```
.aaa
.aarp
.abarth
.abb
.abbott
.abbvie
.abc
.able
```

## Criando uma lista de TLDs

Anteriormente vimos diversos sites que nos auxiliavam na listagem de possíveis TLDs, agora vamos usar o [tlds-from-a-z](#) por ser o mais completo.

Podemos criar um arquivo **.txt** com os domínios e com o passar do tempo adicionando novos que forem encontrados durante o nosso trabalho ou até alguma atualização com TLDs novos.

Agora vamos alterar nossa lista e adicionar domínios que não estão na lista com foco no brasil, por exemplo **.gov.br**, podemos ver que não aparece esse domínio e seria interessante adicionar. Domínios **.gov** acabam não aparecendo e é interessante adicionar. Por exemplo:

- sp.gov.br
- mg.gov.br
- pb.gov.br
- es.gov.br
- pa.gov.br
- rj.gov.br
- ba.gov.br

- ap.gov.br
- se.gov.br
- ce.gov.br
- go.gov.br
- df.gov.br
- rr.gov.br
- sc.gov.br

Todas essas informações podem ser interessantes em algum momento da pesquisa, vai que um domínio governamental está sendo usado como phishing.

## 10. Criando domínios

### Criando domínios gratuitos

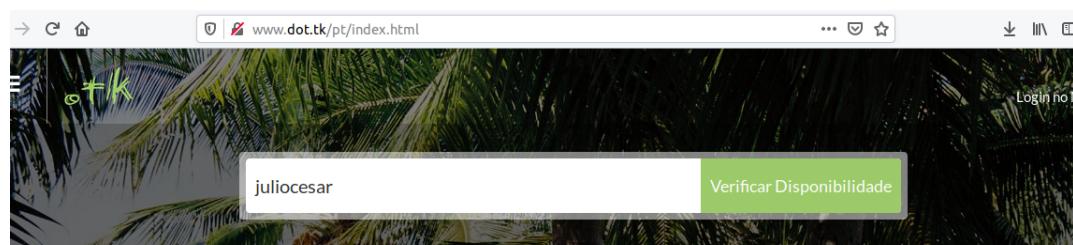
Devido a facilidade em criar novos domínios muitas campanhas são criadas utilizando domínios gratuitos, devido a facilidade ou até não ter gastos para iniciar a operação.

#### Dominios .tk

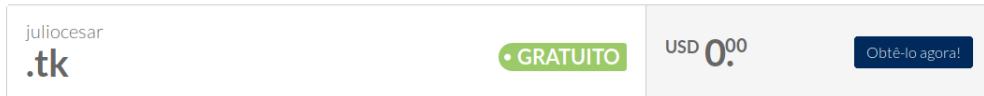
##### Criação de domínio

Vamos usar o projeto dot.tk que é gratuito, mas temos a opção pagar.

<http://www.dot.tk/pt/index.html>



Consiga um destes domínios. Eles são **gratuito!**



Podemos ver que está disponível nosso endereço

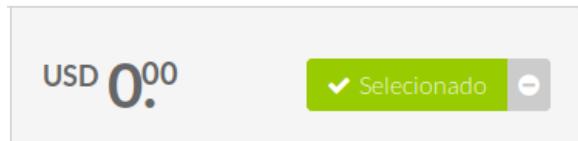
- juliocesar.tk

Vamos clicar em **Obtê-lo agora!**.

Em seguida podemos ir em **Pagamento**.

1 domínio no carrinho Pagamento

!to!



Depois de clicar em pagamento vamos ser redirecionados para

A screenshot of the Freenom website. At the top, there is a navigation bar with links for Services, Partners, About Freenom, Support, Sign in, and English. Below the navigation is a search bar with the placeholder "Find a new FREE domain" and a blue "Check Availability" button. Underneath the search bar, there is a form for domain registration. It includes fields for "Domain" (julioscesar.tk), "IDSHIELD" (with a shield icon), "Use your new domain", "Forward this domain" (with a link icon), "or" (with a link icon), "Use DNS" (with a link icon), "Period" (set to "3 Months @ FREE"), and a "Continue" button.

Em seguida, vamos clicar em **Continue** e vamos ser redirecionados para a seguinte página.

A screenshot of the Freenom "Review &amp; Checkout" page. It shows a summary of the purchase: "Domain Registration - julioscesar.tk" with a price of "\$0.00USD", "Subtotal" of "\$0.00USD", and a "Total Due Today" of "\$0.00USD". Below the summary, there is a field for entering an email address with the placeholder "Please enter your email address and click verify to continue to the next step". There is also a "Verify My Email Address" button. On the right side, there are links for "Already Registered? Click here to login" and "Use social sign in" with options for Google and Facebook, and a "Continue with Facebook" button.

Podemos inserir o email ou se cadastrar com uma conta google. Vou inserir meu email **greenmind.sec@gmail.com** e clicar em **Verify My Email Address**.

Please enter your email address and click verify to continue to the next step

greenmind.sec@gmail.com

Verify My Email Address

Vamos ver no email a confirmação, vamos clicar no link que recebemos em seguida.



Dear customer,

Before completing your order, please confirm your email address by pressing the following link:

<https://my.freenom.com/cart.php?a=checkout&emailverify=H4BTL0CVKJDWEPQA9Y7FS2R61U3N5GXOIZM>

[visit our website](#) | [log in to your account](#) | [get support](#)

Copyright © Freenom. All rights reserved.

Depois vamos ser redirecionados para a página de cadastro, vamos precisar inserir algumas informações, como:

- Nome
- Sobrenome
- Nome da empresa
- Endereço 1

## Review & Checkout

Description	Price
Domain Registration - Juliocesar.tk	\$0.00USD
Subtotal:	\$0.00USD
<b>Total Due Today:</b>	<b>\$0.00USD</b>

### Your Details

First Name	
Last Name	
Company Name	

Além disso precisamos colocar

- Código postal
- Cidade
- País
- Estado
- Número de telefone
- Email
- Senha
- Confirmar senha

Zip Code	
City	
Country	U.S.A.
State/Region	Choose One...
Phone Number	+1
Email Address	greenmind.sec@gmail.com
	<input type="button" value="Change"/>
Password	
Confirm Password	

Tax may be charged depending upon the state and country selections you make. Click to recalculate after making your choices.

I have read and agree to the Terms & Conditions

Não podemos esquecer de aceitar **I have read and agree to the Terms & Conditions**.

City	Bauru
Country	Brazil
State/Region	São Paulo
Phone Number	+55 14 997010196
Email Address	greenmind.sec@gmail.com
	<input type="button" value="Change"/>
Password	*****
Confirm Password	*****

Tax may be charged depending upon the state and country selections you make. Click to recalculate after making your choices.

I have read and agree to the Terms & Conditions

Em seguida, vamos clicar em **Complete Order**.

Se der tudo certo vamos ser redirecionados para a página **Order Confirmation**.

# Order Confirmation

Thank you for your order. You will receive a confirmation email shortly.

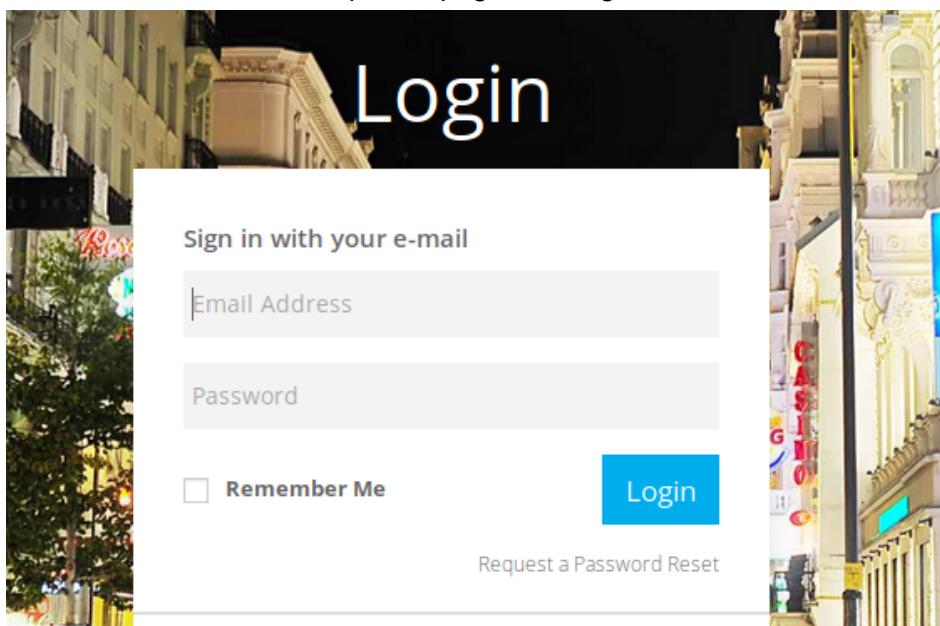
Your Order Number is: 3985416862

If you have any questions about your order, please open a support ticket from your client area and quote your order number.

[Click here to go to your Client Area](#)

Vamos clicar em **Click here to go to your Client Area** para serem redirecionados para a Área do cliente.

Vamos ser redirecionados para a página de login.



Vamos ser redirecionados para a página de login com o DNS padrão.

A screenshot of the Freenom World website. The top half of the page features a vibrant photo of a busy street market with many colorful signs. Below the photo, there's a 'NEW' badge, the 'freenomworld' logo, and a tagline: 'Freenom World is a fast and anonymous Public DNS resolver'. To the right, there's a section titled 'CHANGE YOUR DNS TO' with two input fields containing '80.80.80.80' and '80.80.81.81'. On the far right, there's a video player showing a woman in a red dress speaking. At the bottom, there are links for 'WHY FREENOM WORLD?' and 'WATCH VIDEO'.

## Criando domínios pagos

### Super Domínios

Podemos ver uma lista de domínios disponíveis que podem ser usados para seus sites e que infelizmente caso tenham dinheiro é possível comprar.

<b>.com.br</b> R\$ 35,99 R\$ 44,99	<b>.top</b> R\$ 6,99 R\$ 22,99	<b>.fun</b> R\$ 4,77 R\$ 84,99	<b>.info</b> R\$ 21,99 R\$ 112,99
<b>.biz</b> R\$ 28,99 R\$ 99,99	<b>.link</b> R\$ 4,99 R\$ 59,99	<b>.xyz</b> R\$ 5,79 R\$ 61,99	<b>.CLUB</b> R\$ 37,99 R\$ 103,99
<b>site</b> R\$ 22,99 R\$ 111,99	<b>.online</b> R\$ 40,99 R\$ 137,99	<b>.LIVE</b> R\$ 17,99 R\$ 76,99	<b>.design</b> R\$ 78,99 R\$ 288,99
<b>.social</b> R\$ 44,99 R\$ 177,99	<b>.tech</b> R\$ 59,99 R\$ 177,99	<b>.guru</b> R\$ 17,99 R\$ 202,99	<b>.store</b> R\$ 49,99 R\$ 217,99

Vamos supor que estamos buscando um domínio para realizar uma campanha de phishing usando a imagem do badbank.com.br.

### Registrar Domínio

Encontre o seu novo domínio. Digite seu nome ou palavra-chave abaixo para verificar a disponibilidade.

badbank.com

Procurar

Desculpe, badbank.com não está disponível :-(



Por mais que os domínios .com.br, .net, .com e .org estejam indisponíveis é possível usar o TLD .info para realizar a construção de um domínio **badbank.info**.

# 11. Cybersquatting

## Cybersquatting e Typosquatting diferença

### Algumas variantes de ataque

#### URL - Adição

No ataque de **adição de URL** ou **addition** é realizada a adição de caracteres, dessa forma quando o usuário digita ou até mesmo recebe um phishing via email acaba não percebendo.

Simulando em nosso lab iremos ter o domínio oficial chamado **badbank.com.br**, no caso da adição seria adicionado um caracter por exemplo **baddbank.com.br** ou **badbbank.com.br**.

#### URL - bitsquatting

No ataque de **bitsquatting** é realizada a troca de caracteres, dessa forma quando o usuário digita ou até mesmo recebe um phishing via email acaba não percebendo. Ele se baseia em erros de inversão de bits que ocorrem durante o processo de fazer uma solicitação de DNS, mas na minha visão ele funciona igual ao **URL - Replacement** que também substitui caracteres.

Simulando em nosso lab iremos ter o domínio oficial chamado **badbank.com.br**, no caso da bitsquatting seria trocado um caracter ou mais. Veja mais no exemplo **bedbank.com.br** ou **badbenk.com.br**.

#### URL - Dicionário

No ataque de **dicionário de URL** ou **dictionary** é realizada a adição de palavras, dessa forma quando o usuário digita ou até mesmo pesquisa esse endereço na internet pode se passar por um serviço válido quando na verdade é um phishing. Vamos simular abaixo como funciona esse tipo de ataque.

Simulando em nosso lab iremos ter o domínio oficial chamado **badbank.com.br**, no caso do dicionário de URL seria adicionado uma palavra por exemplo **portalbadbank.com.br** ou **rhbdbank.com.br**.

#### URL - homoglyph

O homoglyph são caracteres que quando visualizado parece determinada letra, mas na verdade não.

Abaixo podemos ver uma solução web onde podemos criar.

- <https://www.irongeek.com/homoglyph-attack-generator.php>

## Homoglyph Attack Generator

homographs based on Homoglyphs than having to search for look-a-like character in Unicode, then coping and pasting. Please use only for legitimate pen-test purposes and user authentication attacks in their code. This is still a work in progress, so please send me suggestions (especially for new Homoglyphs to add). While this tool was designed with making IDNA t can be used for other things. Try ignoring the IDNA/Punycode stuff and just making look alike user names for systems that accept Unicode. I made this tool to easily generate homographs like a lot of modern browsers have gotten better at warning the users of attack, but I'd love to hear experiences about other apps that accept Unicode/Punycode/Internationalized Domain Names.

[Out of Character: Use of Punycode and Homoglyph Attacks to Obfuscate URLs for Phishing](#).

1st, type in a name to look like:

2nd, choose homoglyphs to use:

3rd, Output will be something like this:

4th submit so PHP can generate the IDNA/Punycode:

Unicode URL to give out: βAdbank  
Encoded label to set up in DNS: xn--Adbank-9sa

Abaixo os resultados.

- **Unicode URL to give out:** βAdbank
- **Encoded label to set up in DNS:** xn--Adbank-9sa

Outros links

- <https://github.com/sebob/homographs>

## URL - omission

No ataque de **omissão de URL** ou omission é realizada a remoção de caracteres, dessa forma quando o usuário digita ou até mesmo recebe um phishing via email acaba não percebendo. Vamos simular abaixo como funciona esse tipo de ataque.

Simulando em nosso lab iremos ter o domínio oficial chamado **badbank.com.br**, no caso da omission seria adicionado um caracter por exemplo **bdbank.com.br** ou **badank.com.br**.

## URL - repetition

No ataque de **repetição de URL** ou repetition é realizada a adição de caracteres, dessa forma quando o usuário digita ou até mesmo recebe um phishing via email acaba não percebendo. Vamos simular abaixo como funciona esse tipo de ataque.

Simulando em nosso lab iremos ter o domínio oficial chamado **badbank.com.br**, no caso da repetição de URL seria adicionado um caracter por exemplo **baadbank.com.br** ou **badbaank.com.br**.

## URL - replacement

No ataque de **substituição de URL** ou **replacement** é realizada a mudança de carácter, dessa forma quando o usuário digita ou até mesmo recebe um phishing via email acaba não percebendo. Vamos simular abaixo como funciona esse tipo de ataque.

Simulando em nosso lab iremos ter o domínio oficial chamado **badbank.com.br**, no caso da substituição de URL seria retirado um caractere por exemplo **baddank.com.br** ou **batbank.com.br**.

## URL - subdomain

No ataque de **subdomínio** ou **subdomain** é realizada a criação de parte dos carácter e criado um subdomínio. Podemos ver abaixo como funciona esse tipo de criação.

Simulando em nosso lab iremos ter o domínio oficial chamado **badbank.com.br**, no caso do subdomínio seria adicionado parte no subdomain por exemplo **ba.dbank.com.br** ou **ba.dbank.com.br**.

## URL - tld-swap

No ataque de **troca de TLD** ou **TLD Swap** é realizada a substituição do TLD, já vimos anteriormente o que é **TLD**, nesse ataque altera o TLD responsável.

Simulando em nosso lab iremos ter o domínio oficial chamado **badbank.com.br**, no caso **TLD Swap** seria adicionado um **TLD** diferente por exemplo **baddbank.biz**, **badbbank.co**, **badbbank.net** ou etc.

## URL - transposition

No ataque de **transposição de URL** ou **transposition** é realizada a mudança de ordem dos caracteres, dessa forma quando o usuário digita ou até mesmo recebe um phishing via email acaba não percebendo. Vamos simular abaixo como funciona esse tipo de ataque.

Simulando em nosso lab iremos ter o domínio oficial chamado **badbank.com.br**, no caso da transposição de URL seria alterando a ordem de um caractere podemos ver um exemplo **bdabank.com.br** ou **babdank.com.br**.

## 12. Monitorando domínios e encontrando domínios disponíveis

### DNSTwist

#### Sobre o projeto

O **DNSTwist** além de ser uma solução incrível para nós que estamos buscando phishings, ele é um ótimo parceiro para quem está buscando criar sites suspeitos. Por padrão ele segue **5 qps(Queries por seconds)**, pode demorar muito, mas é devido o número de requisições por segundo.

- Dependendo do alvo que está buscando, podemos aumentar o número de domínios semelhantes.

#### Link oficial do Projeto

Podemos encontrar esse projeto no github.

- <https://github.com/elceef/dnstwist>

#### Instalando DNSTwist - source code

Caso esteja usando Linux podemos clonar o projeto e compilar usando ele com os seguintes comandos:

```
git clone https://github.com/elceef/dnstwist/
cd dnstwist
pip install .
```

#### Instalando DNSTwist - Docker

Caso esteja usando Docker podemos realizar os seguintes comandos:

```
git clone https://github.com/elceef/dnstwist/
cd dnstwist
docker build -t "greenmind/dnstwist:1" .
docker run -it "greenmind/dnstwist:1" "nome-do-cliente.com.br"
```

#### Instalando DNSTwist - Python PIP

Caso esteja usando Linux mais queira instalar o DNSTwist via PIP podemos realizar a instalação com os seguintes comandos:

```
pip3 install dnstwist
```

## Como usar DNSTwist

Abaixo podemos ver a documentação de como usar o DNSTwist.

- <https://github.com/elceef/dnstwist#quick-start-guide>

Podemos buscar por informações de domínios registrados.

```
$ dnstwist --registered dominio.tld
```

Podemos usar uma lista de dicionários para melhorar a criação.

```
$ dnstwist --dictionary dictionaries/english.dict dominio.tld
```

Além disso é possível aumentar a lista de TLDs disponíveis e assim encontrar ainda mais domínios suspeitos.

```
$ dnstwist --tld dictionaries/common_tlds.dict dominio.tld
```

## Versão web do DNSTwist

Além disso, caso seja necessário realizar uma busca de forma rápida, podemos usar uma solução web.

- <https://dnstwist.it/>

Abaixo podemos ver um exemplo de output que podemos ter da solução web.

google.com		Scan	
Scanned 2288 suspicious domains. Identified 342 registered: download as <a href="#">CSV</a> or <a href="#">JSON</a>			
PERMUTATION	IP ADDRESS	NAME SERVER	MAIL SERVER
google.com 	209.85.203.100 2a00:1450:400b:c01::65 United States	ns1.google.com	smtp.google.com
google0.com 	199.59.243.221 United States	ns1.bodis.com	
google1.com 		ns1.googledomains.com	
google2.com 		ns1.googledomains.com	
google3.com 		ns1.googledomains.com	

## URLCrazy

O URLCrazy é uma solução que utiliza técnicas de OSINT para gerar e testar erros de digitação, variações de domínios para detectar ou até executar erros de digitação. Além disso, podemos testar sequestro de URL, phishing e até espionagem corporativa.

## Instalando URLCrazy

Podemos realizar a instalação do projeto usando o gerenciador de pacotes APT nos sistemas Kali Linux, Ubuntu e Debian.

```
$ sudo apt install urlcrazy
```

```

└$ sudo apt install urlcrazy
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libgc-dev libpython3.9-dev python3.9-dev ruby2.7
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libruby3.0 ruby ruby-async ruby-async-dns ruby-async-http ruby-async-io ruby-async-pod
  ruby-protocol-http ruby-protocol-http1 ruby-protocol-http2 ruby-sqlite3 ruby-timers ri

```

## Casos de uso

Alguns casos de uso em que podemos realizar o uso do URLCrazy.

- Conseguimos detectar pessoas má intencionadas lucrando com erros de digitação em seu nome de domínio;
- Tenha a visibilidade e proteja sua marca registrando erros de digitação populares;
- Identifique nomes de domínio com erros de digitação que receberão tráfego destinado a outro domínio;
- Podemos encontrar nomes de domínios que podemos utilizar em ataques de phishing durante pentests.

## Algumas opções de uso

Podemos usar a versão default da seguinte forma:

```
$ urlcrazy badbank.com.br
```

Type	Type	Type	Domain	IP	Country	NameServer	MailServer
<b>Original</b>			<b>badbank.com.br</b>				
Character Omission			babank.com.br				
<b>Character Omission</b>			<b>badank.com.br</b>				
Character Omission			badbak.com.br				
<b>Character Omission</b>			<b>badban.com.br</b>				
Character Omission			badbnk.com.br				
<b>Character Omission</b>			<b>bdbank.com.br</b>				
Character Repeat			baabank.com.br				
<b>Character Repeat</b>			<b>badbaank.com.br</b>				
Character Repeat			badbankkk.com.br				
<b>Character Repeat</b>			<b>badbannk.com.br</b>				
Character Repeat			badbbank.com.br				
<b>Character Repeat</b>			<b>baddbank.com.br</b>				

Por exemplo, caso estejamos realizar um ataque a empresa proprietária do domínio badbank.com.br, poderíamos utilizar alguns dos domínios abaixo para realizar a criação da campanha.

Character Omission	babank.com.br
<b>Character Omission</b>	<b>badank.com.br</b>
Character Omission	badbak.com.br
<b>Character Omission</b>	<b>badban.com.br</b>
Character Omission	badbnk.com.br
<b>Character Omission</b>	<b>bdbank.com.br</b>
Character Repeat	baabank.com.br
<b>Character Repeat</b>	<b>badbaank.com.br</b>
Character Repeat	badbankkk.com.br
<b>Character Repeat</b>	<b>badbannk.com.br</b>
Character Repeat	badbbank.com.br
<b>Character Repeat</b>	<b>baddbank.com.br</b>

Ou até outro TLD.

Homoglyphs	
Wrong TLD	<b>baclbank.com.br</b>
Wrong TLD	<b>badbank.aaa</b>
Wrong TLD	<b>badbank.aarp</b>
Wrong TLD	<b>badbank.abarth</b>
Wrong TLD	<b>badbank.abb</b>
Wrong TLD	<b>badbank.abbott</b>
Wrong TLD	<b>badbank.abvvie</b>
Wrong TLD	<b>badbank.abc</b>
Wrong TLD	<b>badbank.able</b>
Wrong TLD	<b>badbank.abogado</b>
Wrong TLD	<b>badbank.abudhabi</b>
Wrong TLD	<b>badbank.ac</b>
Wrong TLD	<b>badbank.academy</b>

É possível selecionar o tipo de keyboard que será usado, por exemplo:

- qwerty
- azerty
- qwertz
- dvorak

Por padrão podemos usar o tipo **qwerty**.

\$ urlcrazy -k qwerty badbank.com.br

All SLD	<b>badbank.tm.cy</b>
All SLD	<b>badbank.tm.za</b>
All SLD	<b>badbank.tur.ar</b>
All SLD	<b>badbank.tv.tr</b>
All SLD	<b>badbank.vic.au</b>
All SLD	<b>badbank.w.er</b>
All SLD	<b>badbank.wa.au</b>

Podemos realizar a busca apenas por domínios que não foram registrados.

\$ urlcrazy -r badbank.com.br

Original	<b>badbank.com.br</b>
Character Omission	<b>babank.com.br</b>
Character Omission	<b>badank.com.br</b>
Character Omission	<b>badbak.com.br</b>
Character Omission	<b>badban.com.br</b>
Character Omission	<b>badbnk.com.br</b>
Character Omission	<b>bdbank.com.br</b>
Character Repeat	<b>baabank.com.br</b>
Character Repeat	<b>badbaank.com.br</b>

## phishing\_catcher

Projeto oficial

Link do repositório oficial do projeto.

- [https://github.com/x0rz/phishing\\_catcher](https://github.com/x0rz/phishing_catcher)

## O que é o phishing\_catcher ?

Com o phishing\_catcher phishing é possível detectar possíveis domínios de phishing quase em tempo real, isso é possível devido ao projeto procurar por criação de certificados TLS suspeitas relatadas ao **Certificate Transparency Log (CTL)** por meio da **API CertStream**.

## Instalando o phishing\_catcher

Podemos instalar o phishing\_catcher usando o código fonte dele que está disponível no link a seguir:

```
$ git clone https://github.com/x0rz/phishing_catcher
$ cd phishing_catcher
$ sudo pip3 install -r requirements.txt
```

## Como usar o phishing\_catcher?

Podemos usar o phishing\_catcher de forma simples, só chamar o arquivo com o python3.

```
$ python3 catch_phishing.py
```

```
[!] Suspicious: www.pgmil.net (score=1/8)
[+] Potential : 730c45d9-cb13-42ba-99a8-66011e97fa6c.gamma.forgeapps.ec2.aws.dev (score=68)
[+] Potential : run-delete-app-5-run-delete-test-3f7891e2.gamma.forgeapps.ec2.aws.dev (score=76)
[+] Potential : 1.d2.1619410981-cep.cb-gclb-test-prod.certsbridge.com (score=66)
[+] Potential : 2.d2.1619410981-cep.cb-gclb-test-prod.certsbridge.com (score=66)
[+] Potential : 3.d2.1619410981-cep.cb-gclb-test-prod.certsbridge.com (score=66)
[+] Potential : www.news.blog.blog.dev.secure.shortener.to (score=65)
[+] Potential : www.news.blog.blog.dev.secure.shortener.to (score=65)
[!] Suspicious: outlook.familievanveelen.nl (score=95)
[+] Potential : updated.thevoormanproblem.com (score=73)
[!] Suspicious: outlook.Familievanveelen.nl (score=95)
[+] Potential : device-da717df6-0f41-46a2-9abd-07ccec22654d.remotewd.com (score=65)
[+] Potential : 6a015ce4-ff62-4af0-b6af-2d6c8206e46d.gamma.forgeapps.ec2.aws.dev (score=66)
[!] Suspicious: run-delete-app-eu-north-1-1.run-delete-test-eu-north-1-grxknmx.gamma.forgeapps.ec2.aws.dev
[+] Potential : device-local-5e3d6939-ef4c-4a20-9022-9f1f47fb24fa.remotewd.com (score=69)
[!] Suspicious: \*.ap-southeast-2.es.amazonaws.com (score=97)
[!] Suspicious: 6fl7f3rysbcd3re5m3el7opy7y.ap-southeast-2.es.amazonaws.com (score=114)
[+] Potential : updatejo.com (score=67)
[+] Potential : updatejo.com (score=67)
[+] Potential : 9a45c4f5-3b6a-4881-b68a-b89db96868d6.gamma.forgeapps.ec2.aws.dev (score=67)
[!] Suspicious: run-delete-app-ca-central-1-1.run-delete-test-ca-central-1-zj04ily.gamma.forgeapps.ec2.aws.dev
[+] Potential : 73eade18-54e9-43f6-a018-80e3aca50c98.gamma.forgeapps.ec2.aws.dev (score=67)
[!] Suspicious: run-delete-app-ap-south-1-2.run-delete-test-ap-south-1-iwak0o1.gamma.forgeapps.ec2.aws.dev
[+] Potential : device-local-cad3e94f-fde1-4806-8541-d30700e6646d.remotewd.com (score=69)
[!] Suspicious: \*.us-west-2.es.amazonaws.com (score=95)
[!] Suspicious: xx7shtxalqlx5453fbtzgkkcpv.us-west-2.es.amazonaws.com (score=115)
[!] Suspicious: \*.canary-d776711c4e39.2bxcou.c1.kafka.eu-central-1.amazonaws.com (score=119)
[+] Potential : skycharge.redbit.work (score=68)
[+] Potential : device-local-cad3e94f-fde1-4806-8541-d30700e6646d.remotewd.com (score=69)
```

# 13. Hospedagens

## Hospedagens gratuitas

### Hostinger

- <https://www.hostinger.com.br/hospedagem-gratis>

The screenshot shows the Hostinger website for free hosting. At the top, there's a navigation bar with the Hostinger logo, a language switcher for Portuguese, and a dropdown menu for 'Hospedagem'. Below the header, a large banner features the text 'Hospedagem Grátis' and a countdown timer showing '00 : 05 : 57 : 02' (dia(s) : hora(s) : minuto(s) : segundo(s)). A purple button labeled 'Comece Agora' is prominent. To the right, a 'Hosting Account' section displays a price of 'R\$ 6,99/mês' and icons for Cloudflare, Git, WordPress, MySQL Databases, and phpMyAdmin.

Podemos ver que esse tipo de hospedagem é bem limitada, mas também é possível criar seu site com apenas 7 reais.

This screenshot shows a specific offer for 'Hospedagem de Site Grátis'. It highlights a price of 'R\$ 0,00/mês' for 48 months. A purple button says 'Tenha de graça'. Below, a list compares features: a green checkmark indicates '1 Website', '300 MB de Armazenamento SSD', and 'Unlimited Free SSL'; a red X indicates 'Nenhuma Conta de Email', 'Domínio Grátis', 'Largura de Banda Limitada (3 GB)', 'WordPress Gerenciado', and 'Aceleração WordPress'. A link 'Veja todas as características' is at the bottom.

No final das contas quem é a responsável é a 000WebHost :

- <https://www.000webhost.com/>

## Hospedagens Pagas

### Digital Ocean

- Realização de mudança de IPS

### AWS

- Realização de mudança de IPS

## 14. Configuração de DNS

### DNS no domínio

Para não mostrar qual o seu IP do servidor e além disso gerenciar o seu domínio, podemos usar projetos gratuitos que nos auxiliam para uma maior segurança.

### Cloudflare

Cloudflare é um projeto incrível onde podemos direcionar nossos domínios, dessa forma toda a segurança regras de firewall ou até liberar um domínio para determinado país em específico.

Particularmente é o melhor projeto para usarmos em nossos sites pessoais, empresas e até campanhas de phishing. Muitos sites acabam utilizando essa solução justamente para não expor o IP real do servidor.

Vou dar um exemplo do projeto badbank.com.br.

badbank.com.br  
✓ Ativa

Abaixo informações dos endereços DNS.

## Gerenciamento de DNS para **badbank.com.br**

Pesquisar registros de DNS



Buscar

Avançado

Adicionar registro

Tipo	Nome	Conteúdo	Status do proxy	TTL	Ações
A	badbank.com.br	185.199.108.153	Com proxy	Auto	<a href="#">Editar</a>
A	badbank.com.br	185.199.109.153	Com proxy	Auto	<a href="#">Editar</a>
A	badbank.com.br	185.199.110.153	Com proxy	Auto	<a href="#">Editar</a>
A	badbank.com.br	185.199.111.153	Com proxy	Auto	<a href="#">Editar</a>
CNAME	clientes	labpages-vuln.github.io	Com proxy	Auto	<a href="#">Editar</a>
CNAME	em7583	u26510668.wl169.sendgrid.net	Somente DNS	Auto	<a href="#">Editar</a>
CNAME	s1_domainkey	s1.domainkey.u26510668.wl169...	Somente DNS	Auto	<a href="#">Editar</a>
CNAME	s2_domainkey	s2.domainkey.u26510668.wl169...	Somente DNS	Auto	<a href="#">Editar</a>
CNAME	www	bad-bank.github.io	Com proxy	Auto	<a href="#">Editar</a>

Vou realizar um teste de ping para ver qual o endereço do endereço do badbank.com.br.

```
(kali㉿kali)-[~]
$ ping www.badbank.com.br
PING www.badbank.com.br (104.21.79.134) 56(84) bytes of data.
64 bytes from 104.21.79.134 (104.21.79.134): icmp_seq=1 ttl=57 time=32.3 ms
64 bytes from 104.21.79.134 (104.21.79.134): icmp_seq=2 ttl=57 time=20.6 ms
^C
--- www.badbank.com.br ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 20.584/26.447/32.311/5.863 ms
```

Usando o shodan.io podemos verificar informações do IP que foi retornado.

104.21.79.134

Regular View Raw Data History

General Information

Country	United States
City	San Francisco
Organization	Cloudflare, Inc.
ISP	Cloudflare, Inc.
ASN	AS13335

## Outros

- <https://www.duckdns.org>

# 15. Materiais indexados na internet

Atualmente graças ao motores de busca conseguimos encontrar diversos sites na internet com muita facilidade, é possível encontrar blogs que nos ajudam com notícias, sites de instituições, fóruns para busca por informações e lojas virtuais.

## Motores de busca

Temos atualmente diversos sites que nos auxilia nessa busca, entre os principais estão:

- Google;
- Bing;
- Yandex;
- Duck Duck Go;
- Entre outros.

## Google Dorks

Para um melhor êxito em nossas buscas podemos usar palavras específicas e operadores que nos auxiliam.

- [Podemos ver mais sobre Google Hacking](#)

## Palavras chaves e Dorks

Eu recomendo sempre ser o máximo assertivo nas palavras usadas, vamos focar no nome da marca e o título da página oficial.

Quando encontramos uma página na internet um dos pontos que a grande maioria de páginas possui, são os títulos. Também conhecidos no HTML como **<title>Título da página</title>**.

Para realizar a busca por títulos podemos usar o operador:

intitle

```
intitle:"Nome do titulo"
```

Para buscar por algo específico podemos usar o operador "**nome**", dessa forma é possível buscar por uma frase específica.

- "palavras chaves"

O operador site vai nos retornar resultados de um site específico, por exemplo:

```
site:badbank.com.br
```

Já o operador - é negação, ele vai recusar qualquer resultado que esteja no **-site**.

Operador -site

Agora podemos somar informações do título de uma página oficial, negando o site verdadeiro e analisando os resultados em busca de páginas suspeitas.

```
intitle:"Nome do titulo" "badbank" -site:badbank.com.br
```

Para finalizar podemos usar informações de uma url específica, por exemplo:

- badbank.com.br/novos-clientes-badbak

```
inurl:novos-clientes-badbak
```

## 16. Redes sociais

### Buscando páginas suspeitas

Devido ao grande uso das redes sociais, muitas empresas decidiram ter a sua identidade na internet, principalmente nas redes sociais. Graças ao excesso de funcionalidades e a facilidade em conseguir suporte das empresas, muitas pessoas estão criando páginas falsas para capturar informações de usuários desatentos. Neste capítulo iremos buscar por páginas nas redes sociais.

#### namechk

O Namechk é um aplicativo web gratuito permitindo que verifique se um determinado nome de usuário está disponível. Atualmente o Namechk realiza a verificação em mais de 98 sites de redes sociais e também verifica domínios.

O site oficial:

- <https://namechk.com/>

Como posso usar o namechk ?

Podemos realizar a verificação de redes sociais e domínios como vimos anteriormente.

Só precisamos adicionar um determinado nome que queremos verificar.

pagseguro

 Não sou um robô

Temos resultados de domínios, caso queira é possível realizar a busca por mais domínios clicando em **Show more**.

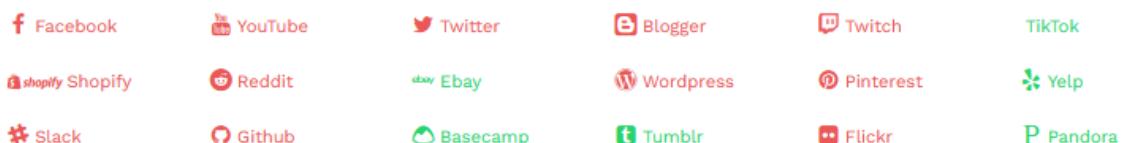
### Domains

pagseguro.com	REGISTERED	pagseguro.net	REGISTERED	pagseguro.me	REGISTERED
pagseguro.org	REGISTERED	pagseguro.us	BUY	pagseguro.info	REGISTERED
pagseguro.la	BUY	pagseguro.asia	BUY	pagseguro.biz	BUY
pagseguro.tv	REGISTERED	pagseguro.ws	BUY	pagseguro.nyc	BUY
pagseguro.okinawa	BUY	pagseguro.online	BUY	pagseguro.network	BUY
pagseguro.ninja	BUY	pagseguro.photo	BUY	pagseguro.photography	BUY

[Show more](#)

Além disso, podemos verificar por possíveis usernames em redes sociais.

### Usernames

[Show more](#)

## Facebook

Com o uso dos operadores é possível realizar a busca por páginas que estão disponíveis e indexadas na internet.

Para realizar a busca por resultados do Facebook podemos usar o operador site seguido do domínio do facebook.

- site:www.facebook.com

Vamos supor que estamos analisando a página pagseguro, ela está no endereço [www.facebook.com/pagseguro](http://www.facebook.com/pagseguro).

Podemos realizar o filtro usando os operadores site e inurl.

- site:[www.facebook.com](http://www.facebook.com) inurl:[pagseguro](http://www.facebook.com/pagseguro)

Aproximadamente 1.510 resultados (0,47 segundos)

<https://www.facebook.com> › ... › Financial service

**PagBank PagSeguro - Home - Facebook**  
PagBank PagSeguro. 1477044 likes · 17248 talking about this · 4 were here. A solução completa em meios de pagamento e serviços financeiros.

<https://www.facebook.com> › pagseguro › posts › está-i...

**Está inscrito no Bolsa Família e vai... - PagBank PagSeguro**  
PagBank PagSeguro is on Facebook. To connect with PagBank PagSeguro, join Facebook today. Join. or. Log In.

Dessa forma podemos pegar características da página oficial e realizar a negação da página oficial.

## Instagram

Podemos filtrar por resultados apenas do Instagram.

- site:[instagram.com](http://instagram.com) inurl:[santanderbrasil](http://santanderbrasil)

Aproximadamente 25 resultados (0,93 segundos)

<https://www.instagram.com> › santanderbrasil

**Santander Brasil (@santanderbrasil) • Instagram photos and ...**  
717k Followers, 19 Following, 2088 Posts - See Instagram photos and videos from Santander Brasil (@santanderbrasil)

<https://www.instagram.com> › channel · Traduzir esta página

**Santander Brasil (@santanderbrasil) • Instagram photos and ...**  
717k Followers, 19 Following, 2089 Posts - See Instagram photos and videos from Santander

Podemos realizar a negação da página oficial e usar características da página para buscar por outras similares.

- site:[instagram.com](http://instagram.com) -inurl:[santanderbrasil](http://santanderbrasil) Santander



site:instagram.com -inurl:santanderbrasil Santander



Todas Maps Notícias Imagens Videos Mais Ferramentas

Aproximadamente 257.000 resultados (1,07 segundos)

<https://www.instagram.com/santanderuniversidadesbrasil>  
**santanderuniversidadesbrasil - Instagram**  
57.8k Followers, 19 Following, 575 Posts - See Instagram photos and videos from **Santander**  
Universidades (@santanderuniversidadesbrasil)

<https://www.instagram.com/farolsantander>  
**Farol Santander (@farolsantander) • Instagram photos and ...**  
Farol **Santander**. Somos um centro de cultura, turismo, lazer e gastronomia em SP e em POA, criado para preservar o passado, iluminar o presente e transformar ...

<https://www.instagram.com/santander.global> · Traduzir esta página  
**santander.global - Instagram**  
9618 Followers, 20 Following, 43 Posts - See Instagram photos and videos from **Santander**  
(@santander.global)

## Twitter

Podemos realizar a busca usando o operador site seguido do site do twitter, em seguida podemos usar o operador inurl seguido da página.

- site:twitter.com inurl:santander\_br



site:twitter.com inurl:santander\_br



Todas Maps Videos Imagens Shopping Mais Ferramentas

Aproximadamente 8.350 resultados (0,93 segundos)

[https://twitter.com/santander\\_br](https://twitter.com/santander_br) ▾  
**Santander Brasil (@santander\_br) / Twitter**  
Um novo jeito de conquistar sua casa dos sonhos: Promoção Sua Casa Tá On. A cada compra a partir de R\$10 nas nossas marcas parceiras, você ganha 1 número da ...  
Tweets & replies · Jul 20 · Jul 22

[https://twitter.com/santander\\_br/status](https://twitter.com/santander_br/status) ▾  
**Santander Brasil on Twitter: "O que a gente pode fazer por ...**  
9 de nov. de 2017 — Conversation ; Cristiano Andrade · @cristiano\_and91 · Nov 9, 2017 ; Santander Brasil · @santander\_br · Nov 29, 2017 ; VandersonFlu · @vandersonflu.

Além disso, é possível negar a página original buscando por outras páginas suspeitas.

- site:twitter.com -inurl:santander\_br santander



site:twitter.com -inurl:santander\_br santander



<https://twitter.com/bancosantander> ▾ Traduzir esta página

**Santander (@bancosantander) / Twitter**

No red without yellow Introducing our special edition livery and driver overalls for this weekend's #ItalianGP ...



## Youtube

Com o uso do operador site:[www.youtube.com](http://www.youtube.com) filtramos por resultados do youtube.

- site:[www.youtube.com](http://www.youtube.com)

Para melhor podemos filtrar por uma determinada página usando.

- site:[www.youtube.com](http://www.youtube.com) inurl:user inurl:pagseguro

The screenshot shows a Google search results page with the query "site:www.youtube.com inurl:user inurl:pagseguro". The results are filtered to show only videos uploaded by users whose names contain "pagseguro". There are three video thumbnails displayed:

- PagBank PagSeguro - YouTube**  
Transferências Ted e Pix GRÁTIS E ILIMITADAS  
0:31  
PagBank PagSeguro tem tudo para você  
YouTube · PagBank PagS... 2 dias atrás
- PagBank PagSeguro - YouTube**  
Como vender recarga de celular na Moderninha X, Smart e no super app PagBank  
2:14  
Como vender recarga de celular na Moderninha X, Smart e no super app PagBank  
YouTube · PagBank PagS... 3 dias atrás
- PagBank PagSeguro - YouTube**  
Como vender recarga de celular na Moderninha Pro 2 e Super App  
2:13  
Como vender recarga de celular na Moderninha Pro 2 e Super App  
YouTube · PagBank PagS... 4 dias atrás

Podemos negar a busca pelo endereço oficial e buscar outras páginas que usam o mesmo padrão de nome.

- site:[www.youtube.com](http://www.youtube.com) inurl:user -inurl:pagseguro pagseguro OR PagSeguro

The screenshot shows a Google search results page with the query "site:www.youtube.com inurl:user -inurl:pagseguro pagseguro OR PagSeguro". The results are filtered to show videos uploaded by users whose names contain "pagseguro" or "PagSeguro", excluding the official channel. There are three video thumbnails displayed:

- Sem título**  
Como Ton (T1 Chip, T2 Touch)**Pagseguro** (Minizinha NFC, Minizinha chip 3, Moderninha Plus, Moderninha Pro 2, Moderninha Smart e Moderninha X), Sumup (Sumup ...)
- BoaCompra by PagSeguro - YouTube**  
BoaCompra at Money 20/20 - Interview with Alain Delcourt  
3:48  
BoaCompra by... 8 de jul. de 2022
- BoaCompra by PagSeguro - YouTube**  
Digital Renaissance in Latin America 2022 - BoaCompra & AMI  
1:02:45  
BoaCompra by... 1 de jul. de 2022
- BoaCompra by PagSeguro - YouTube**  
CONNECTING INTERNATIONAL COMPANIES TO...  
1:34  
BoaCompra by... 17 de nov. de 2021

## LinkedIn

O LinkedIn é um rede social com foco em empresas, empregos e network. Muitas empresas possuem páginas oficiais nessa rede social e podemos entrar em outras empresas que possivelmente fazem parte da mesma empresa ou até páginas que se passam por páginas oficiais.

Vamos fazer um teste buscando informações da empresa pagseguro, é possível buscar por páginas usando operadores do Google como vimos anteriormente.

Com o operador site: podemos filtrar somente por páginas do linkedin.

- site:www.linkedin.com

Normalmente as empresas costumam usar o padrão company.

- site:www.linkedin.com inurl:company

Vamos agora retornar apenas a página do pagseguro.

- site:www.linkedin.com inurl:company inurl:pagbank-pagseguro

site:www.linkedin.com inurl:company inurl:pagbank-pagseguro

Todas Notícias Shopping Imagens Videos Mais Ferramentas

Aproximadamente 1 resultados (0,81 segundos)

<https://www.linkedin.com/company/pagbank-pagseguro>

**PagBank PagSeguro - LinkedIn**

As a company owned by the Folha/UOL Group – the Brazilian internet leader – PagSeguro operates as an issuer, acquirer and offers digital accounts, besides ...

Sabendo que a página oficial é a **pagbank-pagseguro**, podemos realizar a negação dessa página e assim buscando outras páginas que possam possuir o mesmo nome.

- site:www.linkedin.com inurl:company -inurl:pagbank-pagseguro pagbank-pagseguro

A screenshot of a Google search results page. The search query is "site:www.linkedin.com inurl:company -inurl:pagbank-pagseguro pagbank-p". The results show several links to LinkedIn company pages for companies like Pagseguro Internet, UOL PagSeguro, Meu pag!, Credisim, and Radarpag. Each result includes a snippet of the company's profile.

site:www.linkedin.com inurl:company -inurl:pagbank-pagseguro pagbank-p X | ☰ 🔎

Todas Notícias Shopping Imagens Vídeos Mais Ferramentas

Aproximadamente 559 resultados (0,95 segundos)

<https://www.linkedin.com/company/pagseguro-internet>  
**Pagseguro Internet - LinkedIn**  
Pagseguro Internet | 218 followers on LinkedIn. Pagseguro Internet is a financial services company based out of Av Brigadeiro Faria Lima, 1384, ...

<https://www.linkedin.com/company/uol-pagseguro>  
**UOL PagSeguro - LinkedIn**  
UOL PagSeguro | 1426 followers on LinkedIn. UOL PagSeguro is an internet company based out of Brazil.

<https://www.linkedin.com/company/meupag>  
**Meu pag! - LinkedIn**  
Similar pages · will bank. Financial Services · **PagBank PagSeguro**. Financial Services. São Paulo, SP · PicPay. Financial Services. São Paulo, São Paulo · Nubank.

<https://www.linkedin.com/company/credisim>  
**Credisim - LinkedIn**  
About us ; Website: http://credisim.com.br/ ; Industries: Financial Services ; Company size: 201-500 employees ; Headquarters: São Paulo, SP ; Type: Privately Held.

<https://www.linkedin.com/company/radarpag>  
**Radarpag | LinkedIn**  
Cielo Rede Stone Getnet Brasil SumUp Zettle by PayPal **PagBank PagSeguro** Safrapay Acqio BEES Brasil C6 Bank Granito Pagamentos Sipag Mercado Pago Fiserv ...

## 17. Comunidades

Uma grande fatia das informações encontradas vem graças às comunidades, muitas delas possuem soluções e parcerias que muitas vezes analisam 24/7 em busca de novas informações. Vou compartilhar algumas comunidades gratuitas e que podemos ter acesso de forma fácil.

- MISP
- OpenPhish
- Outras

### MISP

#### O que é o MISP

O **MISP Threat Sharing** é uma plataforma de inteligência de ameaças de código aberto. O projeto desenvolve utilitários e documentação para uma inteligência de ameaças mais eficaz, compartilhando indicadores de comprometimento. Existem várias organizações que executam instâncias MISP, listadas no site.

#### Como ele pode nos ajudar ?

Temos a possibilidade de criar nossa própria infraestrutura, devido a rica documentação e por ser opensource conseguimos instalar em nosso servidor.

- <https://github.com/MISP/MISP>

## MISP comunidades

O MISP possui diversas comunidades, algumas que apoiam diretamente o projeto e são:

- <https://www.misp-project.org/communities/>

**CIRCL** (Centro de Incidente Response de Bruxelas)

- <https://www.circl.lu/services/misp-malware-information-sharing-platform/>

**CiviCERT** (Computer Incident Response Center for Civil Society)

- <https://civicert.org>

Entre outras comunidades que podemos encontrar no endereço:

- <https://www.misp-project.org/communities/>

## MISP feeds

O **MISP** possui o recurso para adicionar feeds em nosso sistema, os feeds nada mais são que recursos remotos ou locais contendo indicadores que podem ser importados automaticamente para o MISP em intervalos regulares.

Os feeds podem ser estruturados em formato **MISP**, formato **CSV** ou até mesmo formato de texto livre. Você pode importar facilmente qualquer URL remoto ou local para armazenar os dados em sua instância MISP.

Além dos feeds defaults que vem por padrão.

- <https://www.misp-project.org/feeds/>

Temos diversos tipos de feeds, por exemplo Phishing:

- <https://data.phishtank.com/data/online-valid.csv>

Openphish

- <https://openphish.com/feed.txt>

## Phishingtank

O **Phishingtank** é uma comunidade incrível onde podemos realizar a consulta ou adicionar páginas suspeitas.

**Join the fight against phishing**

Submit suspected phishes. Track the status of your submissions. Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

ID	URL	Submitted by
7348984	https://amaicon-updata.vgkhtp.gs/	w0rmw008
7348982	https://redeemphysical.xyz/	cleanmx ✓
7348981	https://obviously-ai.xyz/	cleanmx ✓
7348977	https://hhs.auth-covid-pass.com/convert-er-name.php?ses...	sems
7348976	https://hhs.auth-covid-pass.com/	sems
7348975	http://www.zonaseguravida-bcp.com/	voldemor
7348974	https://amazon.atztex.cn/404.html	w0rmw008
7348973	https://amazon.atztex.cn/	w0rmw008
7348972	https://irs-form-approval19.com/?update	balomish
7348971	https://exodus-wallet.yahoosteles.com/	r3oersec
7348970	http://verify.gov-linkverif.com/r/3wgqCrp	balomish
7348969	https://etremeyisi.hopto.org/	w0rmw008
7348968	https://irs.gov-linkverif.com	balomish
7348967	https://amozan.co.jp/amzocountchop.shop/	w0rmw008
7348966	http://amozan.co.jp/amzocountchop.shop/	w0rmw008

## Como usar o Phishingtank ?

Para um melhor uso é necessário realização da criação de conta e entrar no sistema.

**Please Sign In**

You have attempted to access a page that requires you to be signed in. Please [register](#) or sign in below.

Username

Password

Podemos adicionar phishing indo até o **Add a Phish**.

← → ⌂ ⌂ https://phishtank.org/add\_web\_phish.php

PhishTank is operated by Cisco Talos Intelligence Group

## PhishTank® Out of the Net, into the Tank.

Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account

### Add A Phish

1. Visit our [What is phishing?](#) page to confirm that the suspected phish meets all of the criteria.  
 2. Add a phish using the form below, or even better, submit a phish directly [via email](#).

**Phish URL:**

Copy and paste the URL of the phishing website.

**What is the organization referenced in the email?**

Select an organization... ▾  
 File the phish under the appropriate organization, or select 'other' if it isn't listed.

**Contents of the email:**

Copy and paste the body of the phishing email.

**Submit**

[Need help?](#)

Podemos também pesquisar por páginas suspeitas indo até **Phish Search**.

← → ⌂ ⌂ https://phishtank.org/phish\_archive.php

PhishTank is operated by Cisco Talos Intelligence Group

## PhishArchive

Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account

Phish Archive Search by Targeted Group Search by ASN

### Phish Archive

Valid?	All	Online?	All	Search
ID	Phish URL			
7348992	<a href="https://paanacacesvip.finance/">https://paanacacesvip.finance/</a> added on Nov 12th 2021 8:17 PM			
7348991	<a href="http://paanacacesvip.finance">http://paanacacesvip.finance</a> added on Nov 12th 2021 8:17 PM			
7348990	<a href="https://my.dekySXu?trackingid=H4fgBN5z&amp;signature=newsletter...">https://my.dekySXu?trackingid=H4fgBN5z&amp;signature=newsletter...</a> added on Nov 12th 2021 8:16 PM			
7348989	<a href="https://amazon.ip.namous.shop/">https://amazon.ip.namous.shop/</a> added on Nov 12th 2021 8:15 PM			
7348988	<a href="https://i.wl.co/IU=https%3A%2F%2Fimy.de%2FkySXu?trackingid=H4fgBN5z&amp;s...">https://i.wl.co/IU=https%3A%2F%2Fimy.de%2FkySXu?trackingid=H4fgBN5z&amp;s...</a> added on Nov 12th 2021 8:15 PM			
7348987	<a href="https://my.dekySXu?trackingid=RXUj7fMC&amp;signature=newsletter...">https://my.dekySXu?trackingid=RXUj7fMC&amp;signature=newsletter...</a> added on Nov 12th 2021 8:12 PM			
7348986	<a href="https://i.wl.co/IU=https%3A%2F%2Fimy.de%2FkySXu?trackingid=RXUj7fMC&amp;s...">https://i.wl.co/IU=https%3A%2F%2Fimy.de%2FkySXu?trackingid=RXUj7fMC&amp;s...</a> added on Nov 12th 2021 8:11 PM			
7348985	<a href="https://areaprivate-clientimps.com/">https://areaprivate-clientimps.com/</a> added on Nov 12th 2021 8:09 PM			
7348984	<a href="https://amaicon-updates.vgkftp.gq/">https://amaicon-updates.vgkftp.gq/</a> added on Nov 12th 2021 8:01 PM			
7348983	<a href="http://supportsystemsavinc.com/home/ssl/public_html/ckfinder/userfile...">http://supportsystemsavinc.com/home/ssl/public_html/ckfinder/userfile...</a> added on Nov 12th 2021 8:00 PM			
7348982	<a href="https://redemphysical.xyz/">https://redemphysical.xyz/</a> added on Nov 12th 2021 8:00 PM			
7348981	<a href="https://obviously-al.xyz/">https://obviously-al.xyz/</a> added on Nov 12th 2021 8:00 PM			
7348980	<a href="http://ashkashz.xyz/design/styles/">http://ashkashz.xyz/design/styles/</a> added on Nov 12th 2021 8:00 PM			
7348979	<a href="http://ashkashz.xyz/design/styles">http://ashkashz.xyz/design/styles</a> added on Nov 12th 2021 8:00 PM			
7348978	<a href="https://orusiphoneshop.com/api/user_verification/signin...">https://orusiphoneshop.com/api/user_verification/signin...</a> added on Nov 12th 2021 7:54 PM			
7348977	<a href="https://mhs.auth-covid-pass.com/enter-name.php?sessionid=8TcRCAvn7ZugG...">https://mhs.auth-covid-pass.com/enter-name.php?sessionid=8TcRCAvn7ZugG...</a> added on Nov 12th 2021 7:53 PM			
7348976	<a href="https://mhs.auth-covid-pass.com/">https://mhs.auth-covid-pass.com/</a> added on Nov 12th 2021 7:53 PM			

Além disso, é possível buscar por uma empresa específica.

 PhishTank® Out of the Net, into the Tank.

Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account

Phish Archive Search by Targeted Brand Search by ASN

### Search by Targeted Brand

Targeted Brand:  Valid?  Online?

What are targeted brands?

- These brands were fraudulently represented in phishing submissions.
- Brand targets are identified by the submitter at the time of submission or the PhishTank software, where possible.
- The majority of phishes are listed as Other, meaning no identification was provided.

See a mis-categorized phish?

- If you come across a mis-categorized submission, please flag it on the individual phish page.

submissions.  
of submission or the PhishTank software, where possible.  
identification was provided.

Valid?  Online?

Friends of PhishTank Terms of Use Privacy Contact  
PhishTank is operated by Cisco Talos Intelligence Group (Talos). Learn more about PhishTank or Talos.

All  
ABL  
ABN  
ABSA Bank  
Accurint  
Adobe  
Aetna  
Alibaba.com  
Allegro  
Alliance Bank  
Amarillo  
Amazon.com  
American Airlines  
American Express  
American Greetings  
Americana  
Ameritrade  
ANZ  
AOL  
Apple

E também filtrar por sites que foram validados como phishing.

 PhishTank® Out of the Net, into the Tank.

Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account

Phish Archive Search by Targeted Brand Search by ASN

### Search by Targeted Brand

Targeted Brand:  Valid?  Online?

What are targeted brands?

- These brands were fraudulently represented in phishing submissions.
- Brand targets are identified by the submitter at the time of submission or the PhishTank software, where possible.
- The majority of phishes are listed as Other, meaning no identification was provided.

See a mis-categorized phish?

- If you come across a mis-categorized submission, please flag it on the individual phish page.

Valid?  Online?

Friends of PhishTank Terms of Use Privacy Contact  
PhishTank is operated by Cisco Talos Intelligence Group (Talos). Learn more about PhishTank or Talos.

All  
Valid phishes  
Invalid (not phishes)  
Unknown

E se ainda estão online.

PhishTank is operated by Cisco Talos Intelligence Group.

**Search by Targeted Brand**

Targeted Brand:  Valid?  Online?

What are targeted brands?

- These brands were fraudulently represented in phishing submissions.
- Brand targets are identified by the submitter at the time of submission or the PhishTank software, where applicable.
- The majority of phishes are listed as Other, meaning no identification was provided.

See a mis-categorized phish?

If you come across a mis-categorized submission, please flag it on the individual phish page.

[Friends of PhishTank](#) [Terms of Use](#) [Privacy](#) [Contact](#)  
PhishTank is operated by Cisco Talos Intelligence Group (Talos). Learn more about PhishTank or Talos.

Também podemos realizar o download da lista de domínios válidos que são distribuídos no formato **.csv**. Infelizmente podemos ver a mensagem abaixo devido ao excesso de uso.

You have exceeded the request rate limit for this method.

- https://data.phishtank.com/data/online-valid.csv

Temos diversos formatos para obter o arquivo, sejam eles XML, CSV, PHP e JSON.

#### Format Options

##### XML

<http://data.phishtank.com/data/online-valid.xml>  
<http://data.phishtank.com/data/online-valid.xml.gz>  
<http://data.phishtank.com/data/online-valid.xml.bz2>

##### CSV

<http://data.phishtank.com/data/online-valid.csv>  
<http://data.phishtank.com/data/online-valid.csv.gz>  
<http://data.phishtank.com/data/online-valid.csv.bz2>

##### Serialized PHP

[http://data.phishtank.com/data/online-valid.php\\_serialized](http://data.phishtank.com/data/online-valid.php_serialized)  
[http://data.phishtank.com/data/online-valid.php\\_serialized.gz](http://data.phishtank.com/data/online-valid.php_serialized.gz)  
[http://data.phishtank.com/data/online-valid.php\\_serialized.bz2](http://data.phishtank.com/data/online-valid.php_serialized.bz2)

##### JSON

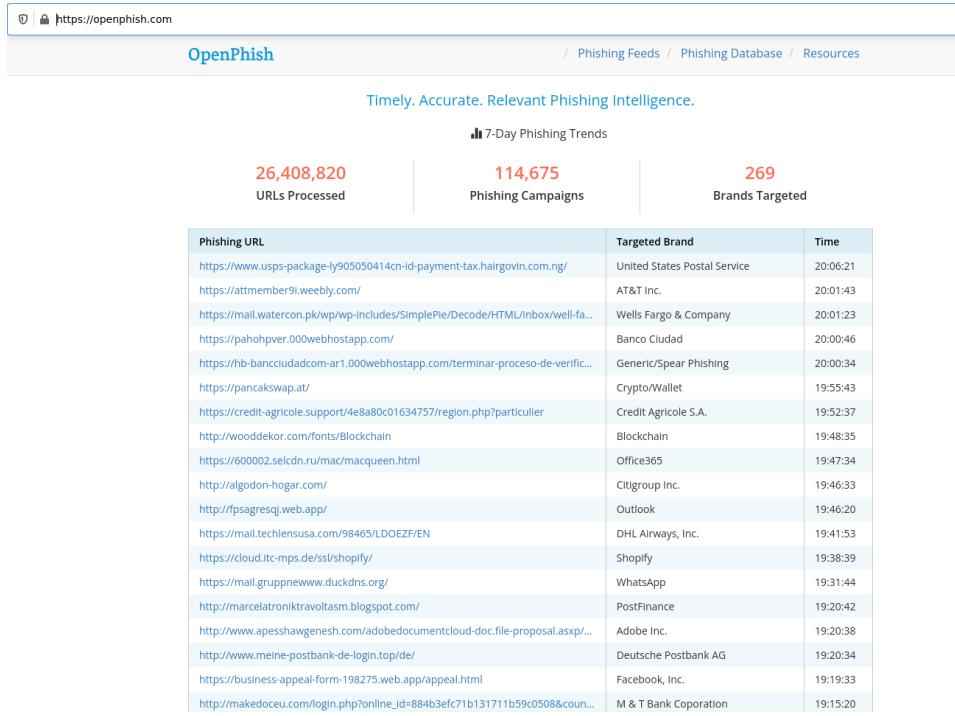
<http://data.phishtank.com/data/online-valid.json>  
<http://data.phishtank.com/data/online-valid.json.gz>  
<http://data.phishtank.com/data/online-valid.json.bz2>

## OpenPhish

### O que é o OpenPhish?

**OpenPhish** é uma plataforma independente totalmente automatizada para inteligência de phishing. Ele identifica sites de phishing e realiza análises de inteligência em tempo real, sem intervenção humana e sem usar recursos externos, como listas negras.

- https://openphish.com/feed.txt



## Outras comunidades

- <https://github.com/mitchellkrogza/Phishing.Database/blob/master/phishing-links-ACTIVEToday.txt>

## 18. Referências

### Referências - O que é a virtualização

Marcela T. G. Santos, Edlane O. G. Alves, Petronio C. Bezerra, Anderson F. B. F. da Costa,  
Um Estudo sobre Migração de Máquinas Virtuais utilizando a plataforma Xen: Instituto  
Federal de Educação, Ciência e Tecnologia da Paraíba - Campus Campina Grande

### Referências - Virtualbox

- [Oracle VirtualBox] (<https://www.virtualbox.org/wiki/>) - 28-08-2018-15:07
- [Linux Download] ([https://www.virtualbox.org/wiki/Linux\\_Downloads](https://www.virtualbox.org/wiki/Linux_Downloads))
- [Old Builds] ([https://www.virtualbox.org/wiki/Download\\_Old\\_Builds](https://www.virtualbox.org/wiki/Download_Old_Builds))

### MISP feeds - Feeds

<https://www.circl.lu/doc/misp/managing-feeds/>

## TLD

<https://br.godaddy.com/blog/tld-o-que-e-quais-existem-e-como-escolher-o-ideal>

O que é TLD - [https://pt.wikipedia.org/wiki/Dom%C3%ADnio\\_de\\_topo](https://pt.wikipedia.org/wiki/Dom%C3%ADnio_de_topo)