Segurança Digital

Um guia prático para se proteger na Internet

Th

Sumário

Introdução

Seja bem-vindo(a) ao guia “Segurança Digital: Um Guia Prático Para se Proteger na Internet”! Se você está lendo este material, provavelmente o encontrou através do meu canal no YouTube ou por alguma divulgação. Neste guia, abordarei como se proteger no ambiente digital, utilizando estratégias eficazes para identificar golpes, verificar a presença de malwares, entender suas diferentes tipologias e estudar o anonimato digital. Cada conceito apresentado aqui transformará a forma como você navega na internet, evitando armadilhas que geralmente capturam usuários menos experientes.

Este guia foi desenvolvido com o objetivo de atingir um público amplo que se interesse pelo tema e deseja melhorar sua segurança e privacidade digital. A minha abordagem será sempre clara e didática, com instruções passo a passo, para que você possa se familiarizar facilmente com os conceitos e, posteriormente, aprofundar seus conhecimentos de forma independente.

Desejo a você ótimos estudos e que este material transforme sua maneira de navegar na internet. Sinta-se à vontade para explorar os temas abordados aqui em outras fontes, como a web, livros e cursos, pois o conhecimento é infinito. Quanto mais você se aprofundar em cada assunto, mais sólido será seu entendimento, deixando-o(a) preparado(a) para enfrentar situações digitais ainda mais complexas.

Obs: Todos os programas mencionados estarão inclusos no Pack de Segurança do guia, basta clicar nesse link que você terá acesso a ele.

A Importância da Segurança Digital

Com o desenvolvimento da tecnologia e o aumento da dependência da internet para realizar nossas tarefas diárias, novas ameaças consequentemente surgiram e têm preocupado cada vez mais os usuários de todos os cantos do mundo. Por esse motivo, os ataques cibernéticos são cada vez mais recorrentes, os quais visam afetar usuários por meio de brechas encontradas nos sistemas de informação desenvolvidos, para roubar dados pessoais, causar danos financeiros, desestabilizar uma rede e entre muitas outras motivações. Neste capítulo, exploraremos a importância da segurança de dados no meio cibernético, os riscos envolvidos e as principais medidas para garantir a segurança das suas informações.

Segurança digital de dados pessoais

Dados pessoais são informações que identificam direta ou indiretamente uma pessoa física na sociedade, são dados únicos, que não podemos ter mais de um indivíduo com os mesmos. Dessa forma, os mais notáveis e importantes que temos são:

- Nome completo;
- Cadastro de Pessoa Física (CPF);
- Carteira de Identidade ou Registro Geral (RG);
- Endereço físico;
- Endereço de IP;
- Senhas;
- Dados bancários (Cartões de crédito);
- Histórico de Navegação;
- Preferências de privacidade.

Esses são apenas alguns dos principais dados pessoas que um usuário da internet tem, ou seja, o acesso inadequado desses por outros indivíduos ou organizações não autorizadas pode gerar uma série de complicações na justiça tanto ao proprietário quanto ao detentor dos mesmos.

O cenário de ameaças no campo cibernético

No mundo digital, os ataques cibernéticos são as principais ameaças de rastreamento de dados não autorizados em todo o mundo. Diversas estratégias são utilizadas por indivíduos mal-intencionados para roubar informações de usuários na rede mundial de computadores.

Entretanto, essas ameaças geralmente afetam dois principais alvos:

- Empresas/Corporações: Nesse caso, os ataques são sempre direcionados à uma empresa em questão, sendo ela o alvo principal desde o início ao fim deles.

  Esses alertas de segurança se mostram evidentes principalmente quando em uma empresa há um ou mais problemas de vulnerabilidade em seu sistema, onde o hacker descobre brechas para invadir ou burlar a proteção estabelecida.

  Entretanto, mesmo sem apresentar problemas de segurança, pode ser que ainda invasores tentarão se infiltrar de alguma maneira.

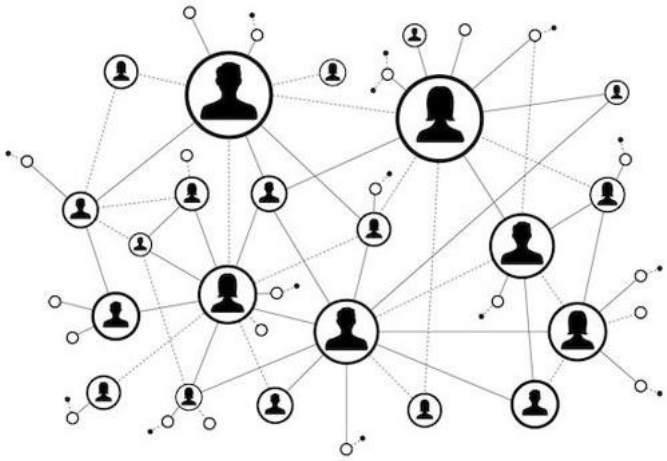
  Os principais efeitos gerados por tais ataques são: roubo de informações confidenciais, interrupções de serviço, prejuízos financeiros, espionagem e fraudes.

- Usuários domésticos: Por outro lado, quando se trata de usuários domésticos estamos tratando de todos utilizadores da internet, os quais os ataques na maioria dos casos não são direcionados especificamente para um alvo (a menos que você tenha um inimigo conhecido que queira te prejudicar virtualmente).

  Geralmente as próprias vítimas caem nesse tipo de golpe, onde é utilizada manipulação e engenharia social por parte do criminoso, por meio do acesso a sites falsos, recebimento de mensagens enganosas ou download de malwares. Mais adiante veremos sobre os ataques cibernéticos mais recorrentes na web.

  Para evitar esses problemas, é necessário simplesmente adquirir novos hábitos de navegação na Internet, evitando cair em armadilhas.

  As principais consequências geradas por esses ataques são: sequestro de dados, espionagem, prejuízos financeiros, danos ao hardware e ameaças reais.



Engenharia Social - Phishing

Engenharia social de forma resumida é uma forma de manipulação psicológica de um indivíduo mal-intencionado para obter informações/dados confidenciais de outra pessoa. Uma das maneiras mais comuns de engenharia social é o Phishing. Veremos neste capítulo como essa técnica funciona, suas variantes e, principalmente, como se proteger desse tipo de ameaça, evitando que seus dados sejam roubados.

O que é Phishing?

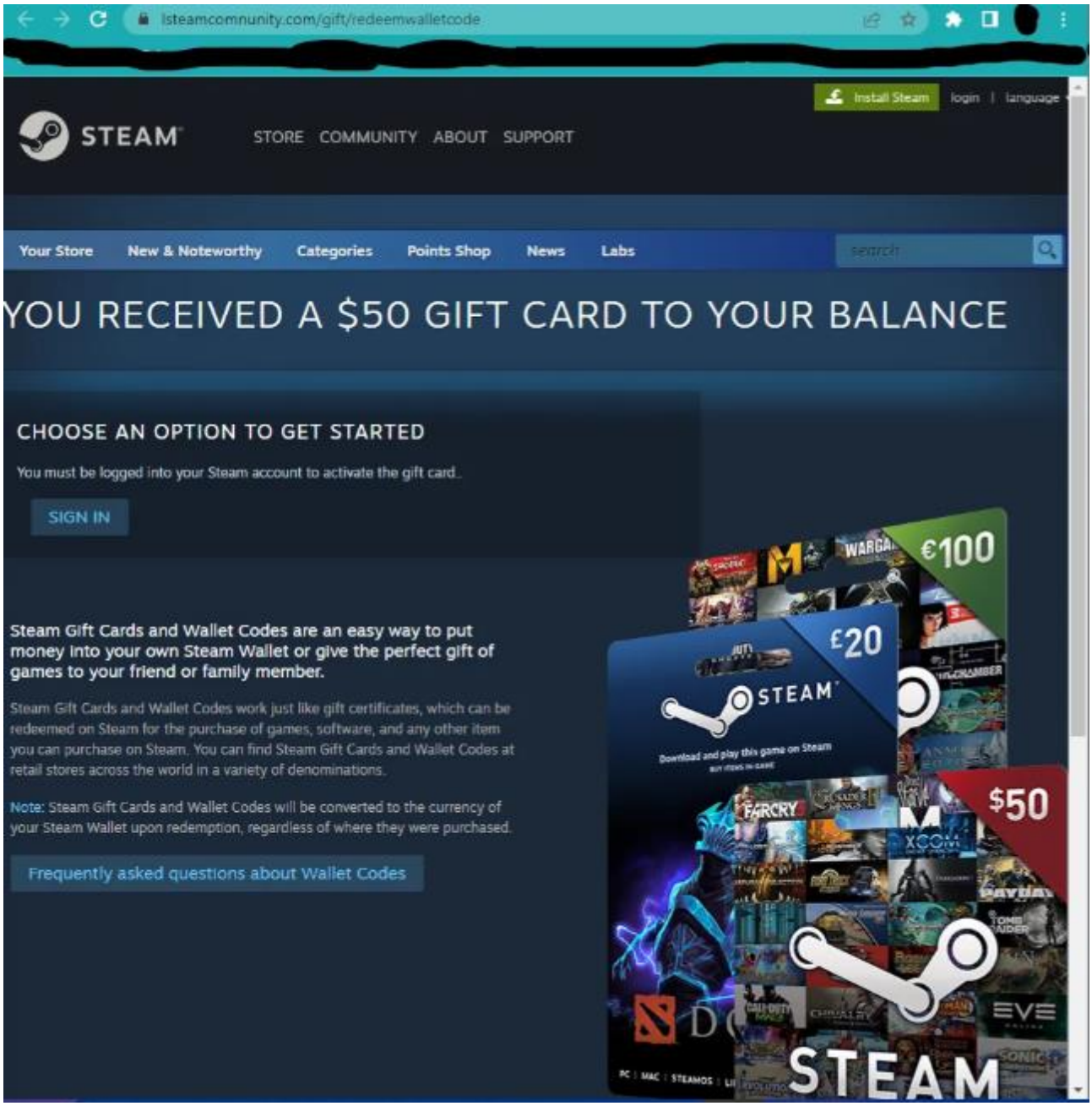
Na Internet, Phishing é um tipo de ataque cibernético em que os criminosos se passam por entidades, organizações ou pessoas confiáveis para persuadir suas vítimas a revelar dados sensíveis, como senhas, informações de contas bancárias ou outros dados pessoais.

Essa técnica pode ser feita de diversas formas, sendo as mais comuns e prováveis realizadas através de comunicações fraudulentas, como mensagens de texto, e-mails ou até ligações telefônicas. O intuito dos criminosos é utilizar de uma argumentação convincente para que a vítima se sinta segura e clique em um link ou baixe um arquivo informado por eles, tendo neles campos para preencher dados como e-mails e senhas, informações bancárias e todo tipo de dados confidenciais desejados extrair de quem caiu no golpe.

Alguns exemplos de aplicações práticas explicadas desse tipo de golpe são:

No caso acima, o golpista envia uma mensagem por e-mail para um vendedor de um produto da plataforma Mercado Livre afirmando que o pagamento pelo produto foi realizado (sendo que não foi) e então pede para que o mesmo seja despachado.

Note que a mensagem de fato parece muito verídica e pode passar despercebida para a vítima, entretanto há algumas coisas para se observar e fazer as devidas verificações: O endereço de e-mail que enviou a mensagem é de fato oficial da plataforma? Há erros gramaticais ou ortográficos presentes no texto? Esse é um modelo de mensagem padrão para todos os vendedores?



Nesse segundo exemplo, temos uma página falsa da loja Steam. Ela diz *"Você recebeu um vale-presente de $50 em seu saldo"*. Bom, aqui já podemos ver uma incongruência: como você recebeu

um presente estando deslogado da sua conta no site? Além disso, é mais improvável ainda que você teria recebido um presente de R$ 285,00 da própria Valve, dona do Steam (a menos que você seja o Gabe Newell).

Depois, o site ainda pede que você logue com sua conta da loja para receber a recompensa, e bom.. Desculpe te decepcionar, mas a única recompensa que você receberá é sua conta sendo desolagada do seu computador depois de um certo tempo e tendo suas credenciais trocadas.

O que acontece aqui é o seguinte: a vítima preenche os campos de login do site com seu usuário e senha da Steam e esses estarão salvos em uma lista com todas os dados das vítimas que caíram no mesmo golpe. Depois o golpista simplesmente poderá acessar sua conta e trocar sua senha, tendo ela agora em sua posse e adeus seus joguinhos...

Assim como a mensagem do “Mercado Livre”, o site em questão também é muito parecido com o do Steam verdadeiro, entretanto é possível fazer observações: O link do website é exatamente idêntico ao do site oficial? O site possui problemas de formatação de texto, como caracteres especiais ou acentos? O site possui ortografia e sintaxe correta? E o mais obvio: Por quais motivos eu receberia um presente do nada e aliás, quem me enviou? Um amigo ou desconhecido? E realmente funcionou para ele? Essas e diversas perguntas podem esclarecer se estamos lidando com algo oficial ou apenas uma tentativa de golpe.

Por fim, temos um exemplo de Phishing muito comum que afeta usuários por meio de mensagens recebidas via WhatsApp, a qual a mesma menciona uma promoção, oferta ou recebimento de valor em sua conta bancária por exemplo. No exemplo acima temos uma promoção do suposto Nubank, dizendo que, devido ao aniversário do banco, você foi um dos 2000 sorteados para receber

um novo cartão de crédito com R$ 12.000,00 de limite, bastando apenas dar alguns cliques e inserir todos seus dados.

Parece uma oferta bastante tentadora, mas infelizmente nada na vida é fácil e temos mais uma tentativa de golpe. Nesse caso, o usuário entraria no link informado e colocaria os seus dados para receber o suposto cartão. Todavia, a empresa oficial do banco foi contatada e afirmou *"Entendo que a oportunidade e a mensagem acaba sendo tentadora, mas é algo fake, combinado?"*.

Entretanto, essa é uma das formas mais fáceis de visualizar de que se trata apenas de um golpe, afinal fica aqui alguns questionamentos: Quais as chances de eu ser um sorteado em um país de 212,6 milhões de habitantes? E ok, supondo que eu sou muito sortudo e realmente tenha ganhado, o próprio aplicativo da Nubank ou via e-mail não poderia me notificar tal surpresa? Uma vez que já tem todos meus dados. Além disso, por qual motivo a mensagem foi encaminhada a mim por um conhecido? Imaginei que se eu realmente tivesse ganhado a empresa pela conta oficial chegaria no meu chat me notificando, não através do número da minha avó.

Identificando um ataque de Phishing

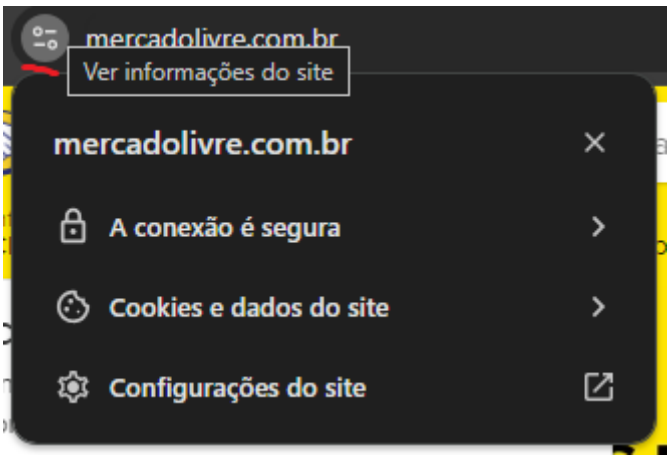
Abordamos nos casos anteriores alguns questionamentos específicos para cada caso, mas agora vamos ver como identificar um golpe do tipo Phishing de forma abrangente.

- Links: A primeira coisa e mais óbvia a se fazer é verificar se o link recebido se trata de fato de uma fonte segura ou não. Em grande parte dos casos, links maliciosos que se passam por uma empresa parecem bastante com a fonte oficial, mas com algum detalhe alterado como um caractere especial, uma letra a mais ou um domínio diferente.

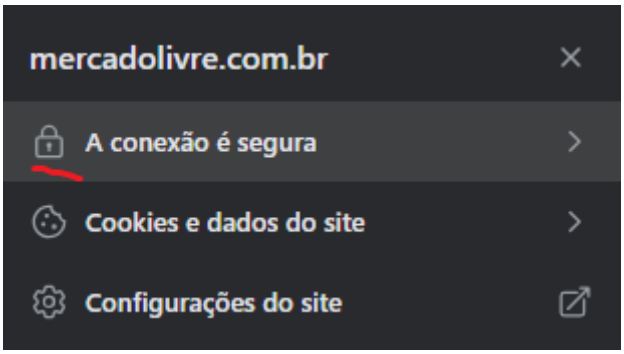
Exemplos de Links falsos	
Oficial	**Phishing**
store.steampowered.com	store.steam**m**powered.com
nubank.com.br	nubank**.net**
amazon.com.br	amazo**n̩**.com.br

Podemos ainda verificar o certificado HTTPS emitido para um site, o qual geralmente sites fraudulentos não sequer possuem.

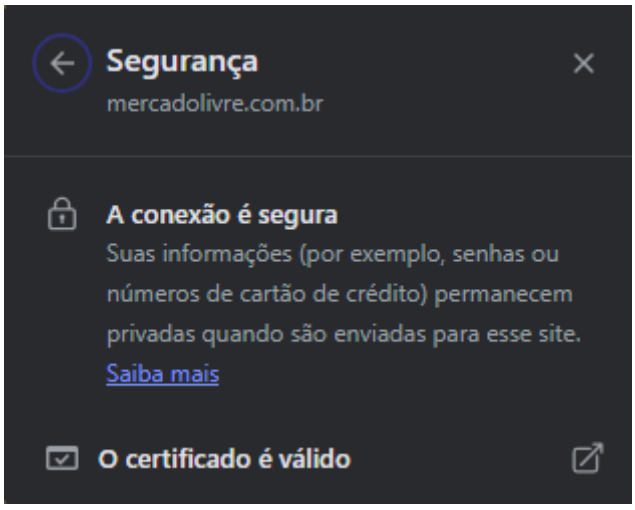
Para fazer isso, iremos no ícone de informações do site ao lado do link



Depois vamos no tipo de conexão do site, clicando na opção com cadeado

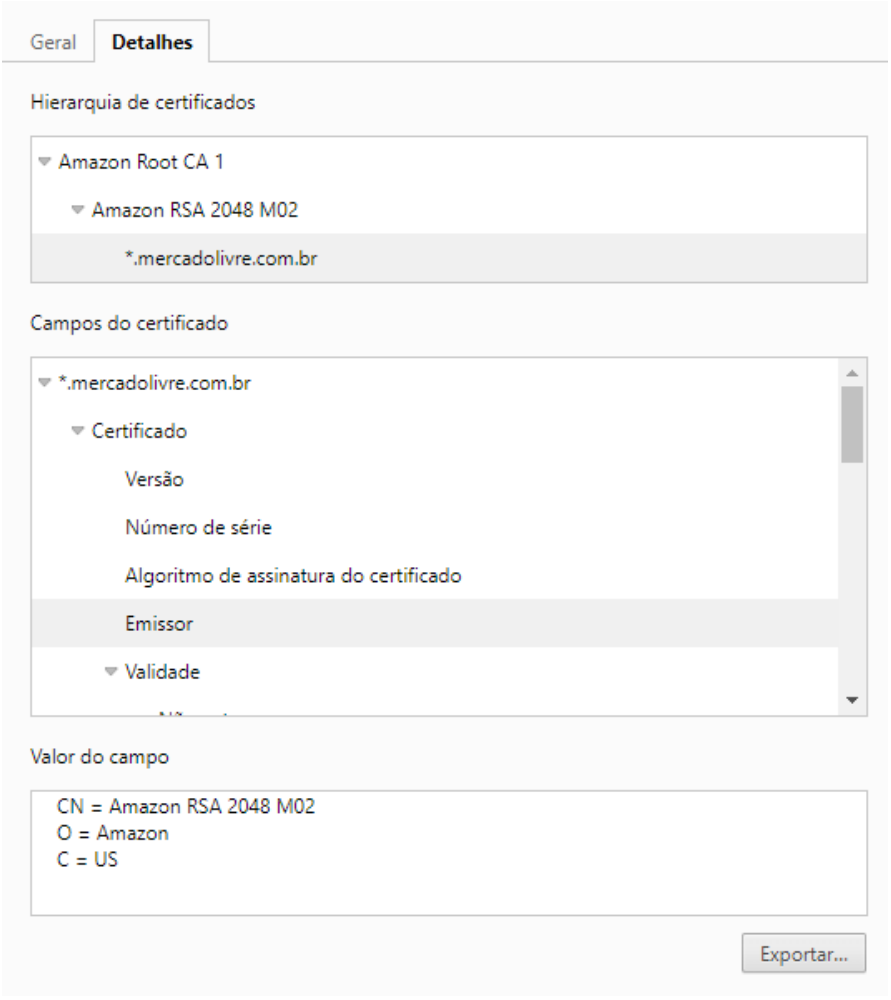


Podemos visualizar a seguinte mensagem, indicando que o site possui um certificado de segurança



Por fim, podemos ainda abrir o certificado emitido para o site, contendo informações sobre a organização e e IDs de identificação do mesmo


Geral
Detalhes
Emitido para
Nome comum (CN) *.mercadolivre.com.br
O (Organização) <Não faz parte do certificado>
Unidade organizacional (OU) <Não faz parte do certificado>
Emitido por
Nome comum (CN) Amazon RSA 2048 M02
O (Organização) Amazon
Unidade organizacional (OU) <Não faz parte do certificado>
Período de validade
Emitido em segunda-feira, 4 de dezembro de 2023 às 21:00:00
Expira em sexta-feira, 3 de janeiro de 2025 às 20:59:59
Impressões digitais SHA-256
Certificado 23863bbb76f3f275fdbfe27125697c1f9b02b59db9c072f1ffeb5d547b85fa2e
Chave pública 914604ae0916c86ddecfaccf5f86b0277bf2e614db6280e0b8efda698850cc83


Geral
Detalhes
Hierarquia de certificados
Amazon Root CA 1
Amazon RSA 2048 M02
*.mercadolivre.com.br
Campos do certificado
*.mercadolivre.com.br
Certificado
Versão
Número de série
Algoritmo de assinatura do certificado
Emissor
Validade
Valor do campo
CN = Amazon RSA 2048 M02
O = Amazon
C = US
Exportar...

- Arquivos: Receber arquivos inesperados por alguém já é um sinal de que tem algo errado, principalmente se tratando de um desconhecido ou um assunto que não foi levantado em momento algum.
  Afinal, por qual razão a Netflix me enviaria um gerador de chaves de assinatura gratuito para sua plataforma?

- Erros gramaticais e ortográficos: É muito comum em páginas da web ou mensagens de texto de caráter enganador possuir em sua escrita erros básicos da língua portuguesa, seja por quais que forem os motivos.
  Por exemplo escrever “mais” ao invés de “mas” ou até palavras escritas erradas da língua da página, como “atensão" ou “vosê”.

- Problemas de formatação de texto: Em um site, utilizamos formatação de texto, que garantem que acentuações ortográficas sejam devidamente exibidas.
  Porém, muitas dessas que são meramente Phishing scams simplesmente não utilizam de formatações como “utf-8” no código HTML da página, ficando com problemas na formatação do texto da página.
  Por exemplo, um texto que era pra ser exibido como “Premiação” sai na verdade como “Premia ├º ├o”.

- Remetentes suspeitos: Receber um e-mail que a primeira vista parece autêntico pode de fato enganar muitas pessoas, mas muitas vezes contém variações quase que imperceptíveis como o domínio do endereço de e-mail alterado, por exemplo: atendimento.mobile@banc0dobrasiloficial.com

- Solicitações de dados pessoais: Se de repente uma empresa que você conhece ou até mesmo faz parte te manda uma mensagem solicitando suas informações pessoais saiba que na maioria dos casos se trata de um golpe.
  Empresas legítimas como bancos, provedores de serviços ou plataformas nunca solicitam dados sensíveis, como senhas ou números de cartões de crédito, via e-mail ou mensagem telefônica.

Mas como se proteger?

Depois de tudo que foi apresentado, conhecemos essa forma de engenharia social, que é o Phishing e como ele é bastante comum e eficaz no mundo cibernético, pois está relacionado à confiabilidade da informação entre seres humanos.

Não há uma forma definitiva para se proteger disso, sempre estaremos vulneráveis, porém podemos utilizar das técnicas de identificação citadas acima para que esclareça as intenções por quem está por trás da mensagem ou link que recebemos.

Além disso, é fundamental que todos adotem uma postura responsável ao fazer uso da Internet, que inclua a educação contínua sobre novas ameaças. Permanecer atento às boas práticas de navegação na internet, como verificar a autenticidade de mensagens e ativar a autenticação em dois fatores das contas pessoais, pode ser a diferença entre ser uma vítima de um golpe ou estar a dois passos à frente do golpista.

Ao adotar essas medidas, conseguimos minimizar consideravelmente o risco de sermos alvo de ataques de phishing, reforçando a proteção dos nossos dados pessoais e financeiros em um ambiente cada vez mais digital.

Malwares e Seus Tipos

Malwares, comumente chamados de vírus de computador, são programas desenvolvidos e projetados por criminosos virtuais para invadir, controlar, danificar ou espionar sistemas operacionais ou redes. Iremos abordar nesse capítulo seus principais tipos, como cada um age e como evitar cair nesse tipo de armadilha.

Esses programas geralmente são instalados pelo próprio usuário do computador, ou seja, a própria vítima é responsável pelos seus atos. Dessa forma, é impossível ter seu computador infectado por algum programa malicioso caso não tenha instalado nada de errado. É importante destacar também que é possível ter um computador ou rede infectada por um malware por meio de dispositivos de armazenamento externos, como pen-drives ou cartões de memória que possuem os arquivos nocivos.

Tipos de Malwares

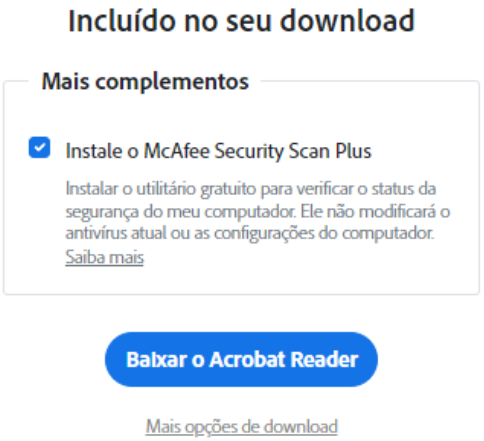
Adwares

Figura 1 - Propagandas enganosas

- O que são: São programas maliciosos que, embora sejam inofensivos ao computador, incomodam o usuário durante o uso de seu computador no cotidiano, prejudicando sua experiência por meio de anúncios e pop-ups exibidos na tela.

- Como são instalados: A instalação deles ocorre em momentos que são instalados outros programas, ou seja, através de instaladores com botões pré-selecionados permitindo sua instalação nas máquinas de usuários menos atentos, onde o mesmo clica “Next” sem perceber que está instalando um monte de porcaria junto. Além disso, pode ser instalado por meio de páginas de download falsas, com botões que direcionam para downloads indesejados.

- Como se proteger: A melhor forma para se proteger dos Adwares é prestando atenção durante os downloads que você faz na internet. Isso vai desde o momento que você clica em um link de download, certificando que de fato é o correto, até o instalador do programa em questão, verificando se há algum programa se instalando junto do desejado.



Além disso, vale também evitar instaladores de terceiros como Baixaki, Softonic ou Softpedia, busque sempre a fonte oficial do programa em questão.
Também é recomendado usar algum bloqueador de anúncios, como os próprios nativos de navegadores como Brave ou Vivaldi, que funcionam bem, ou extensões como adblock.

- Como remover: De modo geral, para remover um Adware a primeira coisa que fazemos é tentar desinstalá-lo pelo painel de controle do Windows ou acessando pastas conhecidas. Caso o programa de alguma maneira não seja desinstalado pelo método convencional, é recomendada a execução de algum scanner específico para a remoção de Adwares, como o software AdwCleaner e HitmanPro (disponíveis no pack de segurança do guia).

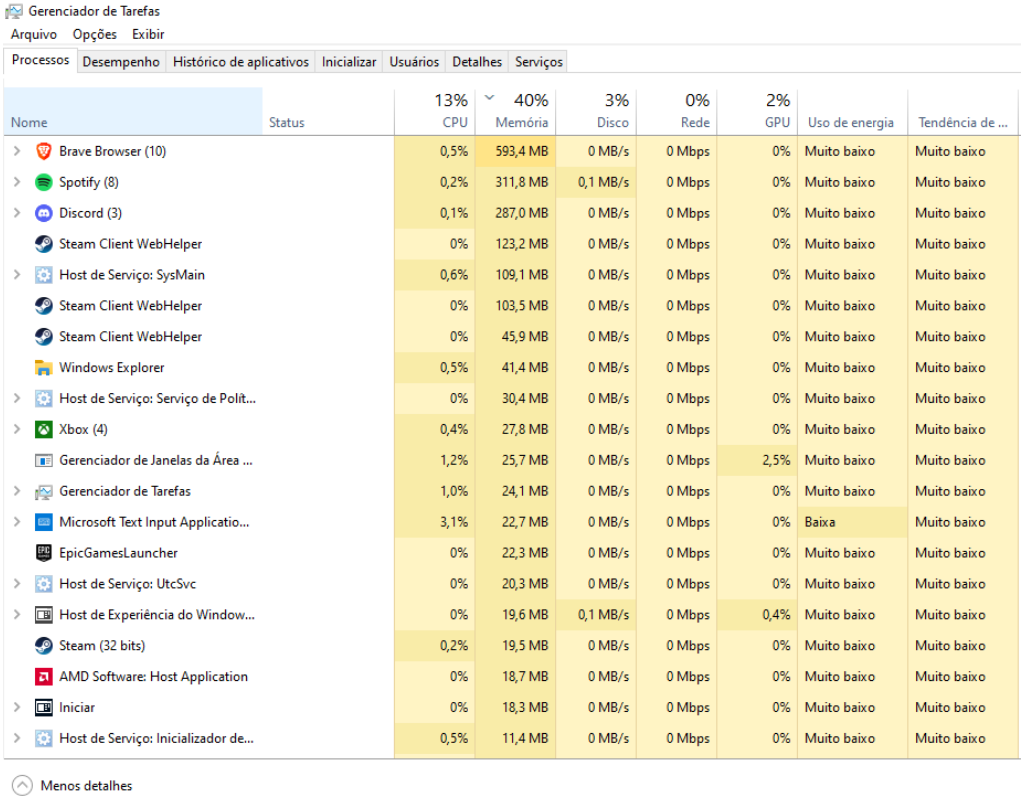
Trojans

- O que são: São programas maliciosos que, diferentemente dos adwares, causam danos diretamente ao sistema. Há diversas motivações pelas quais são desenvolvidos os trojas, existindo diferentes categorias para os mesmos, como veremos a seguir.

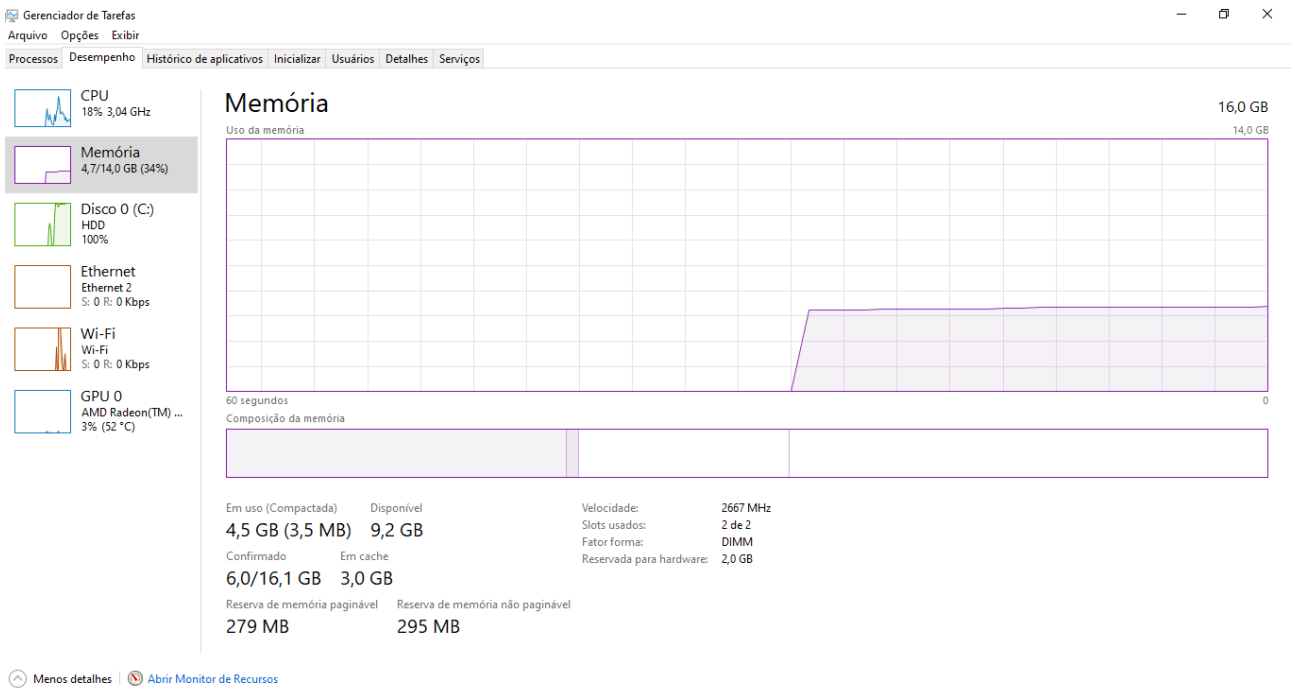
- Categorias dos trojans:
  - ✓ Backdoor: Permite que hackers controlem remotamente o computador da vítima, por meio de um ponto de acesso pela "porta dos fundos", como o próprio nome diz, sem que o usuário perceba sua presença.
  - ✓ Spy: É projetado para espionar o usuário sem o seu conhecimento. Ele monitora atividades como o uso do teclado (keylogging), screenshots, coleta de dados de navegação, e pode até gravar conversas e vídeos se houver microfone e câmera conectados.
  - ✓ Ransom: Realiza o sequestro de dados, os criptografando no computador da vítima e exige que seja realizado um pagamento em criptomoedas para o resgate dos arquivos.
  - ✓ Exploit: Se aproveita de vulnerabilidades ou falhas em um software, sistema operacional ou rede para obter acesso não autorizado, realizar ações maliciosas ou comprometer a segurança de um sistema.
  - ✓ Rootkit: Oculta a presença de outros malwares no sistema e facilita o controle remoto da máquina infectada, tornando difícil para o usuário ou softwares de segurança detectarem suas atividades.
  - ✓ Banker: Focado em roubar dados financeiros dos usuários especificamente, como informações de contas bancárias e credenciais de sistemas de pagamento online.

- Como identificar: Além de alguns comportamentos indesejados apresentados acima, muitas vezes pode ser difícil identificar um trojan. Para isso, podemos analisar os processos do sistema, caso algum seja desconhecido ou suspeito o melhor a se fazer é pesquisar sobre ele em

fóruns ou artigos na internet. Caso note um uso considerável de recursos do seu hardware mesmo sem estar rodando algo “pesado” ou estando em idle, muitas vezes pode ser algo malicioso instalado em seu computador. E é claro, caso seus dados pessoais, contas e dispositivos sofram alguma alteração perceptível, como deslogamentos injustificados, alterações de senhas ou tentativas de login, muito provavelmente você está sendo afetado por algo malicioso.



Nome	Status	13% CPU	40% Memória	3% Disco	0% Rede	2% GPU	Uso de energia	Tendência de ...
Brave Browser (10)		0,5%	593,4 MB	0 MB/s	0 Mbps	0%	Muito baixo	Muito baixo
Spotify (8)		0,2%	311,8 MB	0,1 MB/s	0 Mbps	0%	Muito baixo	Muito baixo
Discord (3)		0,1%	287,0 MB	0 MB/s	0 Mbps	0%	Muito baixo	Muito baixo
Steam Client WebHelper		0%	123,2 MB	0 MB/s	0 Mbps	0%	Muito baixo	Muito baixo
Host de Serviço: SysMain		0,6%	109,1 MB	0 MB/s	0 Mbps	0%	Muito baixo	Muito baixo
Steam Client WebHelper		0%	103,5 MB	0 MB/s	0 Mbps	0%	Muito baixo	Muito baixo
Steam Client WebHelper		0%	45,9 MB	0 MB/s	0 Mbps	0%	Muito baixo	Muito baixo
Windows Explorer		0,5%	41,4 MB	0 MB/s	0 Mbps	0%	Muito baixo	Muito baixo
Host de Serviço: Serviço de Polít...		0%	30,4 MB	0 MB/s	0 Mbps	0%	Muito baixo	Muito baixo
Xbox (4)		0,4%	27,8 MB	0 MB/s	0 Mbps	0%	Muito baixo	Muito baixo
Gerenciador de Janelas da Área ...		1,2%	25,7 MB	0 MB/s	0 Mbps	2,5%	Muito baixo	Muito baixo
Gerenciador de Tarefas		1,0%	24,1 MB	0 MB/s	0 Mbps	0%	Muito baixo	Muito baixo
Microsoft Text Input Applicatio...		3,1%	22,7 MB	0 MB/s	0 Mbps	0%	Baixa	Muito baixo
EpicGamesLauncher		0%	22,3 MB	0 MB/s	0 Mbps	0%	Muito baixo	Muito baixo
Host de Serviço: UtcSvc		0%	20,3 MB	0 MB/s	0 Mbps	0%	Muito baixo	Muito baixo
Host de Experiência do Window...		0%	19,6 MB	0,1 MB/s	0 Mbps	0,4%	Muito baixo	Muito baixo
Steam (32 bits)		0,2%	19,5 MB	0 MB/s	0 Mbps	0%	Muito baixo	Muito baixo
AMD Software: Host Application		0%	18,7 MB	0 MB/s	0 Mbps	0%	Muito baixo	Muito baixo
Iniciar		0%	18,3 MB	0 MB/s	0 Mbps	0%	Muito baixo	Muito baixo
Host de Serviço: Inicializador de...		0,5%	11,4 MB	0 MB/s	0 Mbps	0%	Muito baixo	Muito baixo



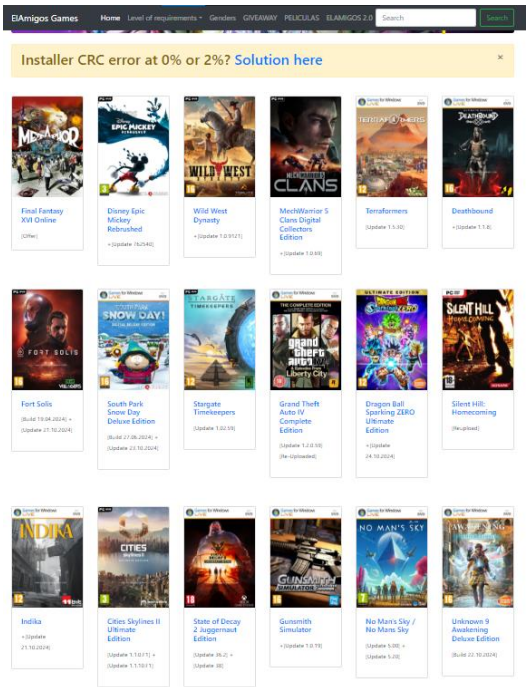
- Como são instalados: Os trojans são instalados de inúmeras formas, por meio de downloads de arquivos alternativos/piratas pela internet, recebimento de anexos de arquivos por mensagens ou redes sociais.

  Como mencionado anteriormente, eles não se instalam sozinhos em seu computador, em 100% dos casos ocorre quando um usuário desinformado faz o download e instala conscientemente me sua máquina, às vezes por ingenuidade ou desconhecimento dos potenciais riscos que aquele software poderia trazer ao seu sistema.

  Quando um trojan é instalado através de outro programa, chamamos essa técnica de "crypter", utilizada para enganar softwares de segurança como antivírus durante o scan dos arquivos.

  Eles também podem aparecer por meio de arquivos baixados de jogos crackeados, onde o executável do jogo original é substituído pelo do pirateado, para que funcione "corretamente", mas por baixo dos panos está sendo executado em segundo plano um trojan em sua máquina.

  Por exemplo hacks de jogos online, que prometem adicionar moedas para sua conta, sendo que na verdade isso é tecnicamente impossível pois a aplicação teria que ter acesso direto ao servidor que estão armazenados os dados das contas dos usuários, portanto não existe cheats que suprem essa função.



- Como se proteger: A principal dica para se proteger dos trojans de modo geral é sempre veri-

ficar a fonte de download de um determinado programa. Escolha por baixar programas sempre de uma fonte que seja confiável.

Mas não vou ser hipócrita de dizer que todos têm condições de pagar R$ 400,00 em jogos em lançamentos e por isso acabamos optando por alternativas secundárias de download, mas mesmo assim existem opções seguras para consumir esses conteúdos, basta pesquisar.

Outro ponto importante a ser mencionado é que a infecção de um computador por um software malicioso só e somente ocorre após o momento que o usuário executa esse programa baixado, portanto, mesmo que você baixe o pior vírus que já foi desenvolvido de toda a humanidade, mas não executou ainda, você está seguro.

Verifique também se a extensão do arquivo baixado corresponde ao esperado, ou seja, caso tenha baixado uma imagem, ela deve corresponder a um arquivo jpeg ou png, por exemplo.

Segue uma lista das principais extensões de arquivos:

Extensões de arquivos	
Texto	.txt, .doc, .docx, .pdf, .rtf, .md, .html
Imagens	.png, .jpg, .jpeg, .gif, .bmp, .webp, .tiff, .tif, .svg, .heif, .heic
Áudios	.mp3, .wav, .aac, .flac, .ogg, .wma, .aiff, .alac
Vídeos	.mp4, .avi, .mkv, .mov, .wmv, .flv, .webm, .mpeg, .3gp
Executáveis	.exe, .bat, .com, .msi, .app, .bin, .run, .sh, .jar

Caso esteja em dúvida em relação a um arquivo, você pode utilizar o site https://virustotal.com para verificar a existência de vírus por diversos bancos de dados de inúmeros antivírus de uma vez, suas relações, parentescos etc.

Além disso, opte também por baixar programas **open source**, este que possuem seu código fonte disponibilizado para que todos possam ver, ou seja, é muito improvável que algo malicioso esteja presente no código, uma vez que muitos programadores têm acesso e sabem identificar se de fato é legítimo ou não. Além disso, eles são gratuitos, tornando-os ferramentas bastante úteis em nosso dia a dia.

No próximo capítulo do nosso guia iremos falar sobre os ambientes controlados, como máquinas virtuais ou caixas de areia, que servem justamente para testar todo tipo de arquivo, sem afetar diretamente o sistema real do indivíduo.

- Como remover: Para realizar a remoção de um trojan que infectou uma máquina, são inúmeras formas para tal, uma vez que depende de cada caso em particular. Dessa forma, uma vez

que foi detectado especificamente qual o trojan afetou o sistema, o ideal seria pesquisar métodos de remoção próprios para ele, através de um software projetado para essa finalidade ou até mesmo manualmente.

Caso desconheça o vírus, o mais óbvio a se fazer é rodar um antivírus confiável e que seja eficaz. Segue uma lista com os melhores softwares para a remoção de malwares:

- ✓ Kaspersky Total Security;
- ✓ Panda;
- ✓ Norton 360;
- ✓ Bitdefender;
- ✓ Spybot – Search & Destroy;
- ✓ Windows Defender.

Mas como falei anteriormente: O verdadeiro antivírus é você mesmo! Não adianta sair comprando as melhores licenças de antivírus sendo que sua navegação na Internet é totalmente irresponsável, faça downloads somente quando de fato precisar!

Ambientes Isolados: Virtualização e Sandboxing

Neste tópico iremos abordar o tema Ambientes Isolados e como eles podem ser poderosos para fazer testes dos mais variados tipos. Vamos aprender a como preparar um sistema virtualizado com o VirtualBox, software poderoso que emula máquinas virtualmente, e como executar programas em um ambiente isolado do sistema operacional principal, criando uma camada de segurança para seu computador utilizando Sandboxing.

O que são Ambientes Isolados?

Ambientes isolados referem-se a métodos de execução onde aplicações podem rodar sem interferir diretamente no sistema principal. Isso é particularmente útil para desenvolvedores, analistas de segurança, e qualquer pessoa que precise testar softwares com segurança, garantindo que sua máquina real não seja afetada.

Assim como vimos nos assuntos anteriores, às vezes baixamos programas e não temos certeza se devemos executá-los ou não, devido seu potencial risco. Dessa forma, utilizando desses artifícios podemos testar com segurança os programas que quisermos.

Virtualização e Sandboxing

- Virtualização: Consiste na criação de uma máquina virtual completa, incluindo sistemas operacionais completos e independentes, possibilitando instalar, configurar e gerenciar isos diversas.

- Sandboxing: Técnica utilizada para isolar a execução de programas específicos/selecionados em um ambiente seguro sem a necessidade de criar um sistema completo. O software opera em uma safe-zone, com limitações de acesso aos recursos críticos do sistema.

Máquinas virtuais: VirtualBox

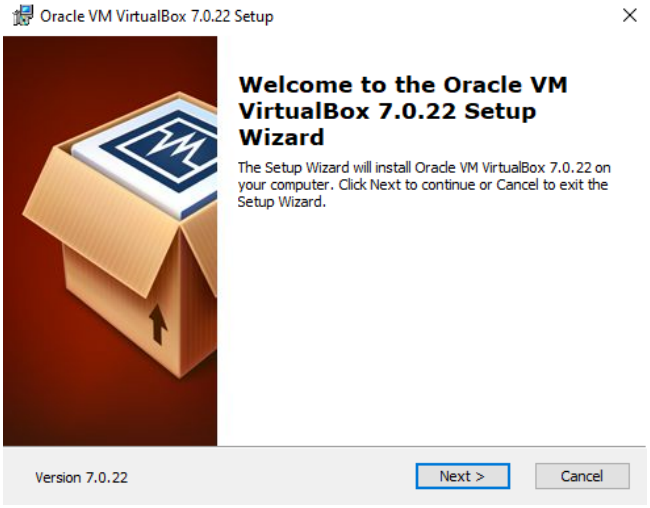
Iremos agora de fato aprender a preparar uma máquina virtual para execução de testes isolados. Há inúmeros softwares para fazer isso, como VMware, mas iremos aprender a utilizar o VirtualBox, da empresa Oracle.

- Instalação: Primeiramente, iremos ao site de download oficial do VirtualBox e baixamos o arquivo de instalação.

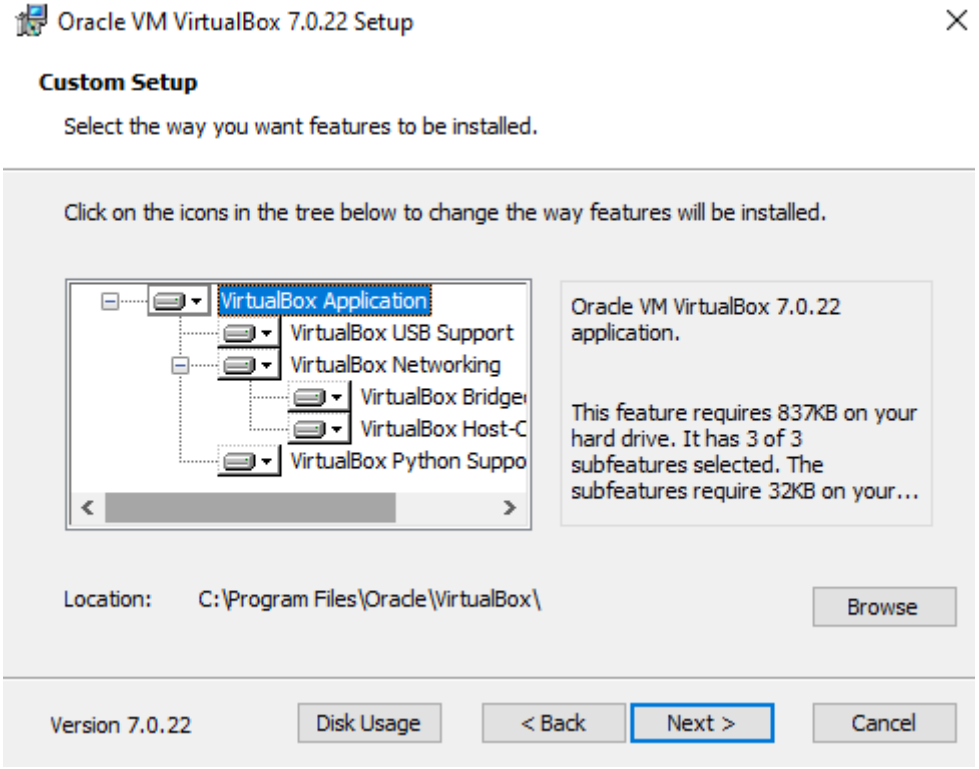
Selecione o download do instalador correspondente ao seu SO

Após baixar, execute o instalador na pasta onde foi baixado

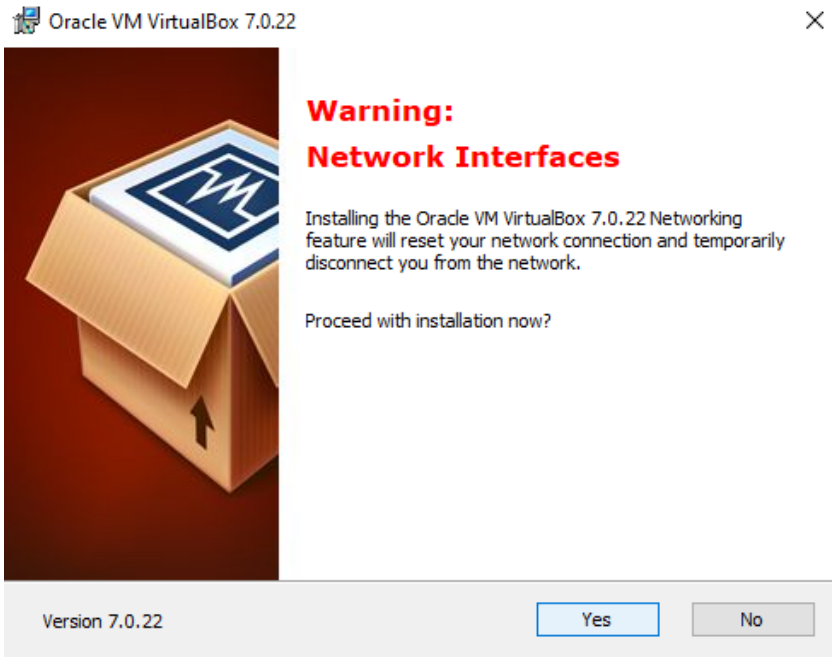
Aqui é o mesmo de sempre... “Next”



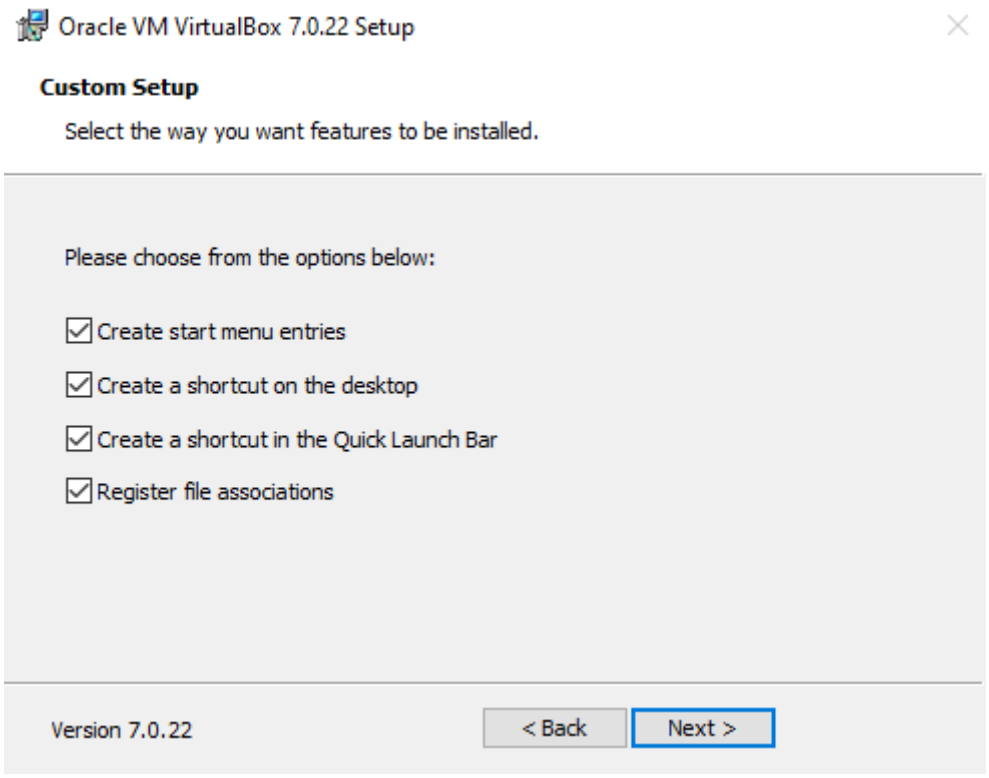
Só altere alguma opção caso queira desativar algum recurso como Rede ou portas USB, caso contrário, prossiga a instalação clicando em “Next”



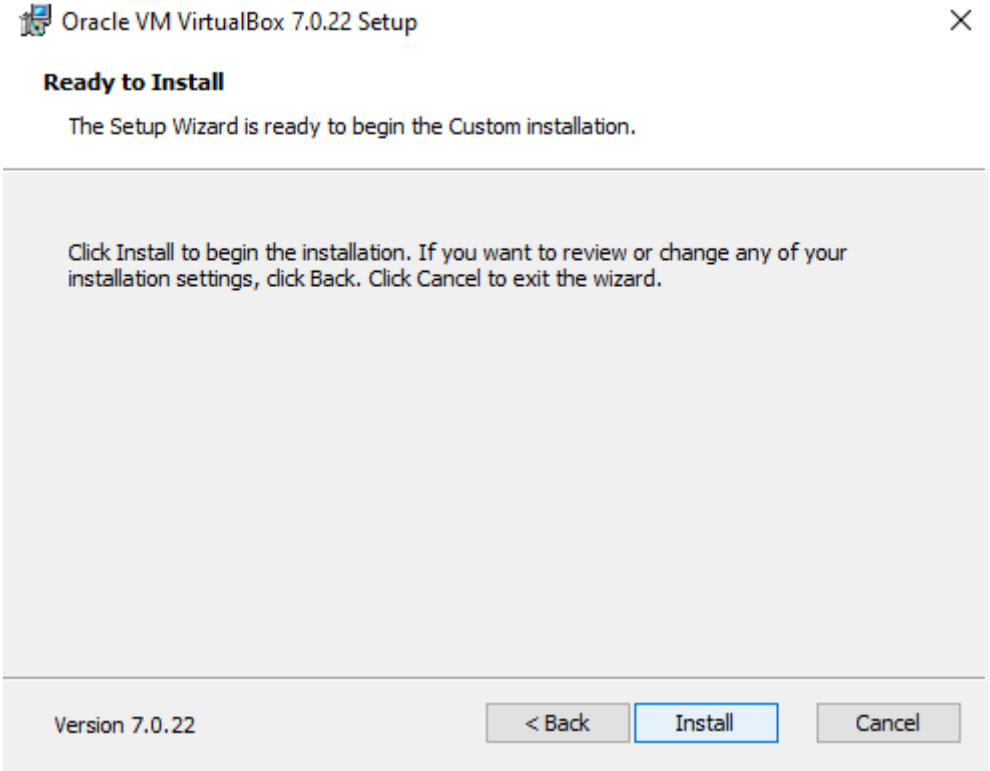
Não se assuste caso sua placa de rede pare de funcionar temporariamente, em alguns segundos ela estará de volta, isso se dá devido a instalação de recursos de rede para o funcionamento de internet na máquina virtual



Selecione a criação ou não de atalhos de acordo com suas preferências



Clique em “Install” e aguarde a instalação ser concluída

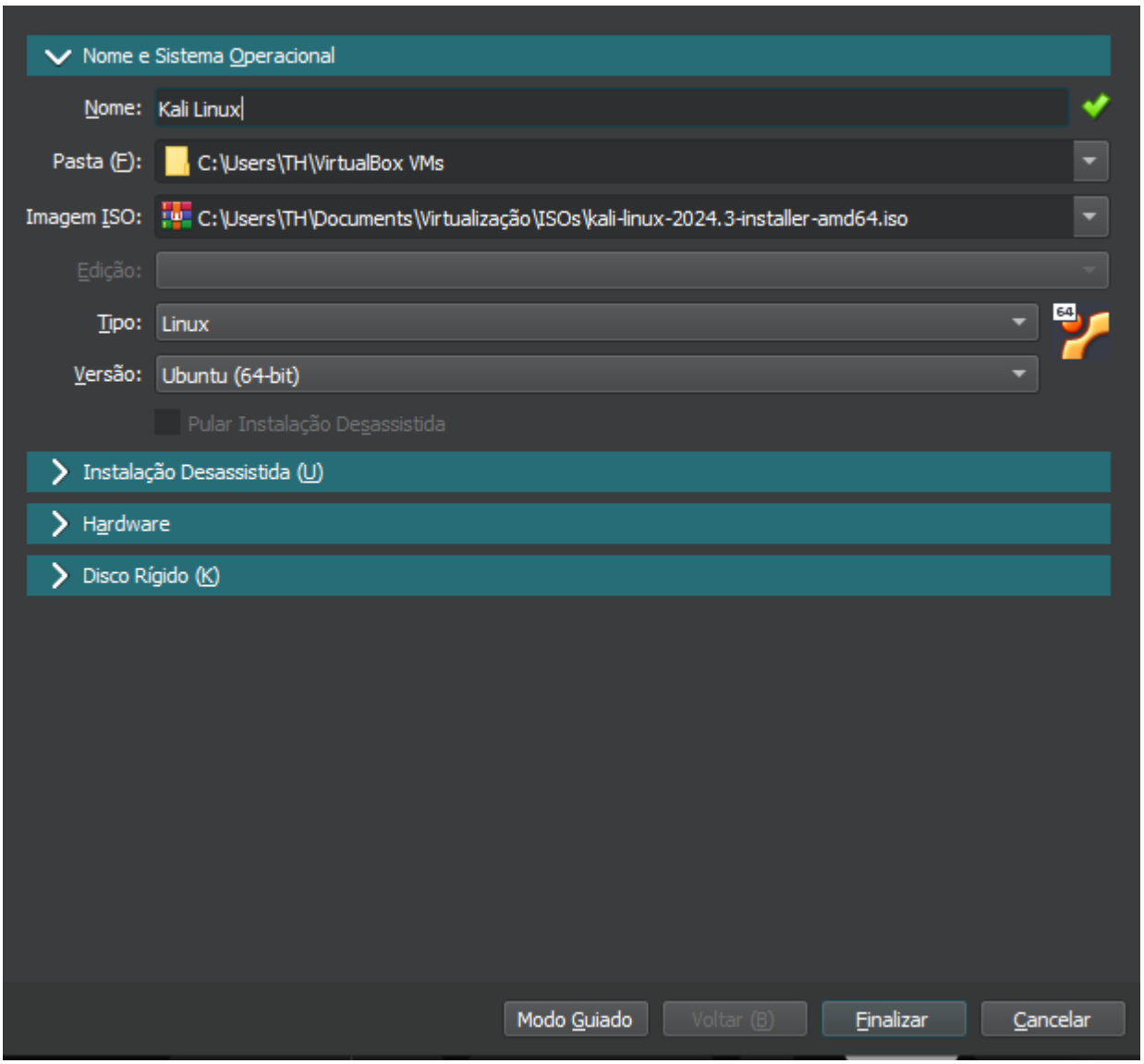


- Download da ISO: Para prosseguir, será necessário baixar uma ISO do sistema operacional desejado (Windows, Linux etc), para que dessa forma possamos criar nossa máquina virtual. Neste guia estarei utilizando a distribuição Kali, do Linux.

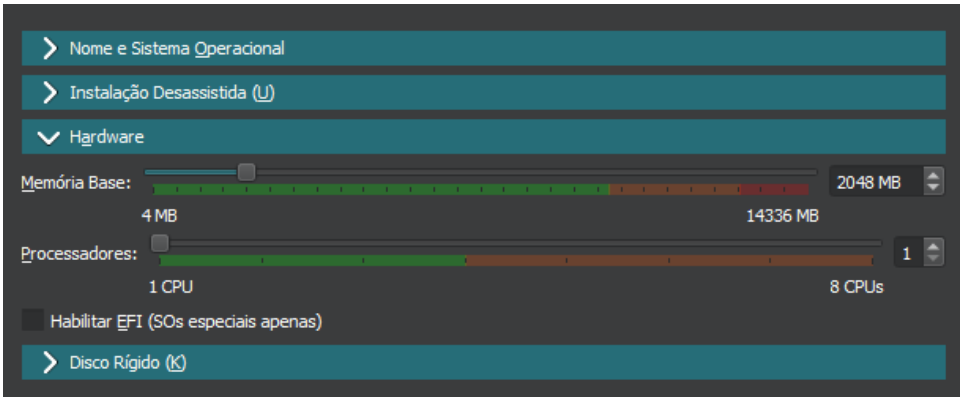
- Criando uma máquina virtual: Depois de baixar, execute o VirtualBox.

Clique em "Novo" e será criada uma nova máquina virtual

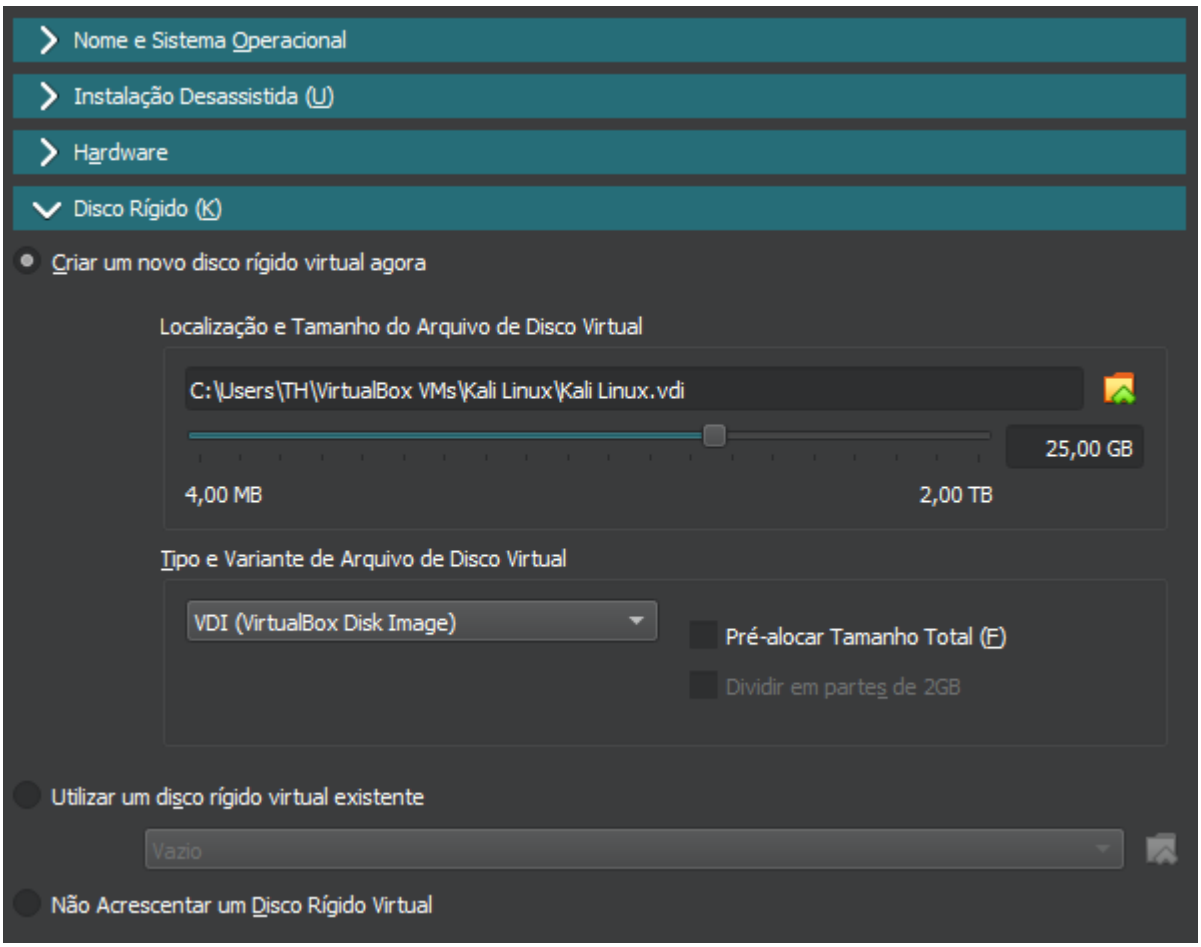
Antes de continuar nessa parte, selecione abaixo a opção "Modo Expert" e você terá a seguinte tela. Digite o nome do sistema operacional, selecione a pasta que será criada a máquina virtual e a ISO baixada. Por padrão serão preenchidos o Tipo e Versão do SO após identificação, confirme se está correto



Na aba de Hardware, escolha valores que estejam dentro da área verde, de acordo com seu hardware para evitar gargalos ou problemas maiores.



Na gua Disco rígido, selecione a quantidade de armazenamento que sua máquina virtual terá, isso varia de acordo com seu hardware e de quantos gigas estão disponíveis em seu sistema. Então clique em “Finalizar”

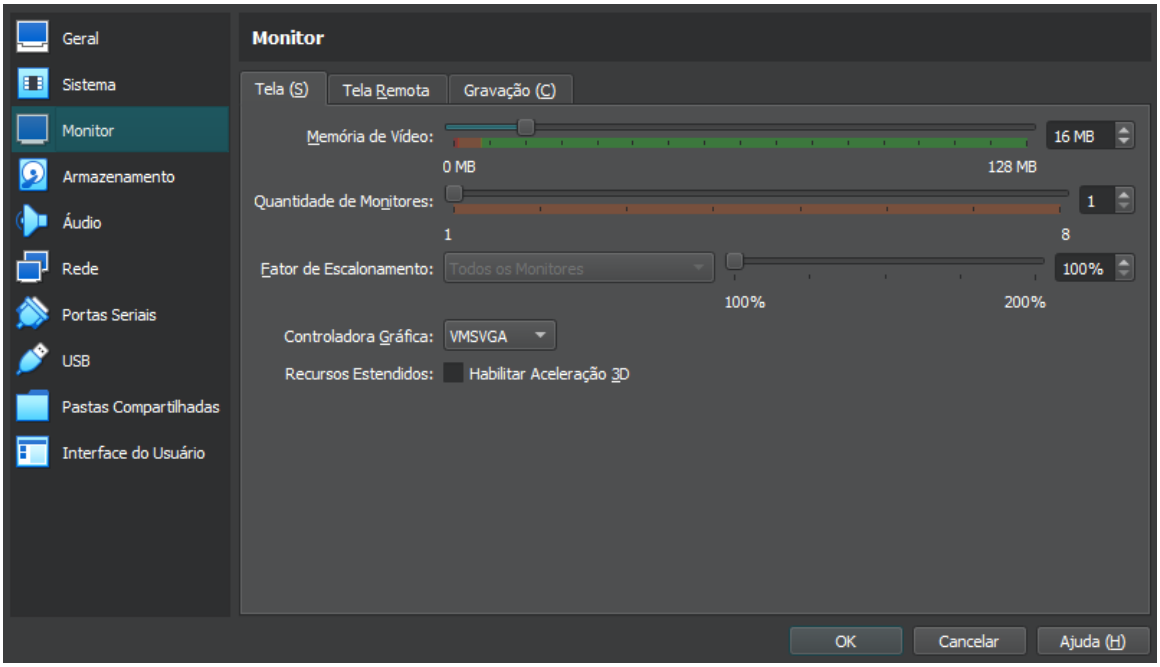


- Configurando a máquina virtual: Após criada, vamos à algumas configurações adicionais da nossa máquina virtual.

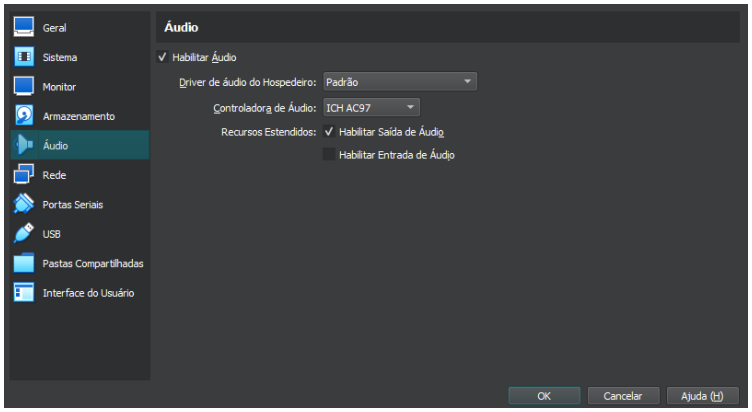
Para isso, clique no ícone de configurações a seguir

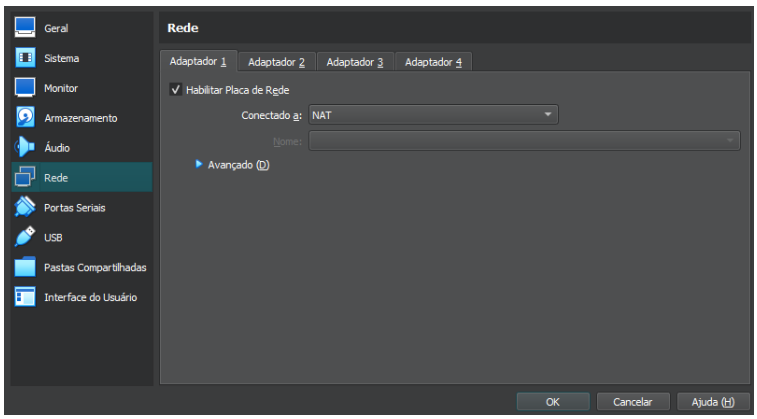
Vamos na aba “Monitor” e podemos alterar a quantidade de memória de vídeo que o SO terá. Novamente, utilize valores que estejam dentro da faixa verde para evitar problemas.

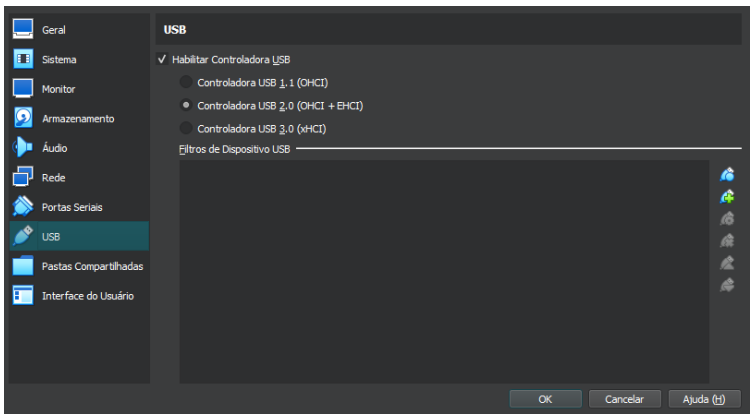
Podemos ainda definir a quantidade de monitores de vídeo que serão utilizados pela máquina virtual.



Por padrão o Áudio, Placa de Rede e Portas USB vêm habilitados, entretanto verifique se as opções estão de fato ativadas.

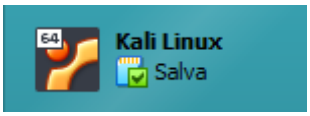






- Inicializando: Por fim, vamos inicializar nossa máquina virtual, após todas essas configurações, prosseguindo para a instalação do SO.

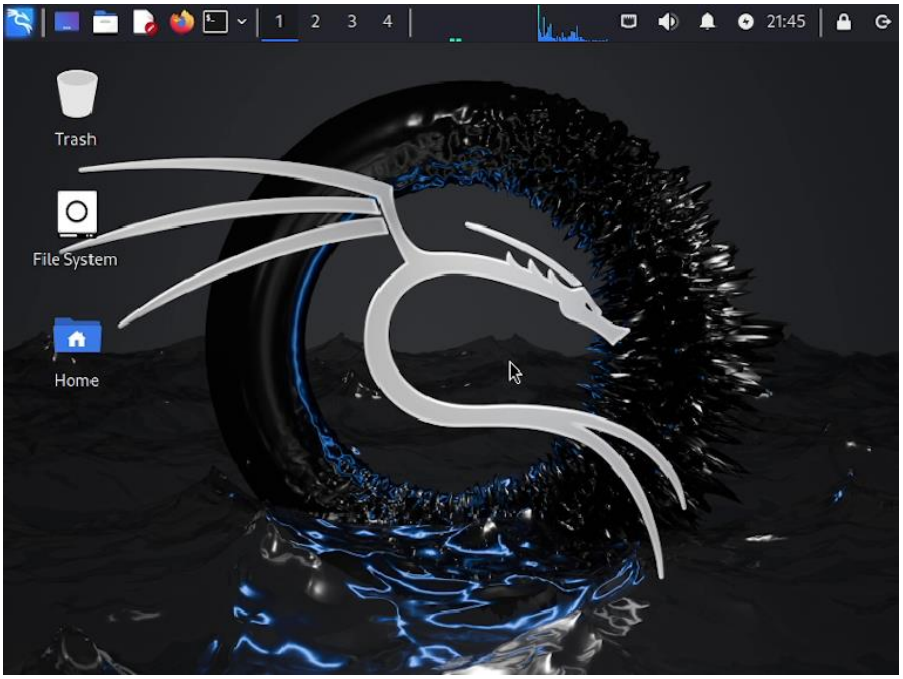
Para ligar nossa máquina, basta dar dois cliques em seu indicador



Será aberta essa janela do VirtualBox, aqui ocorrerá toda a execução da nossa máquina virtual.

Será inicializada a tela de instalação do seu sistema operacional escolhido, basta apenas ir seguindo o passo a passo

Aguarde alguns minutos e seu sistema estará pronto para uso!



A partir deste momento, você está apto para realizar os mais diversos testes em sua máquina virtual.

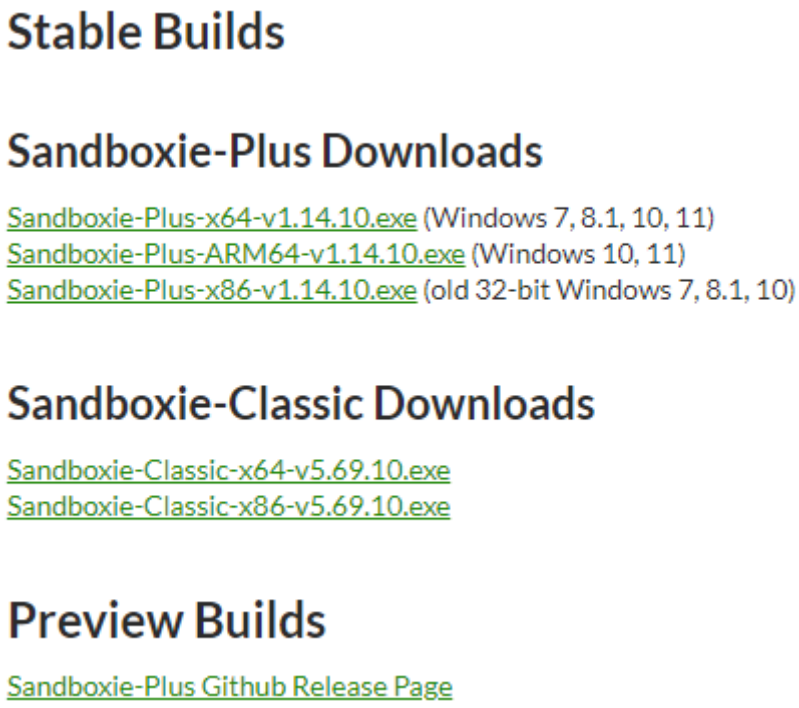
Uma dica: Quando for executar algo duvidoso, desligue sempre a internet da sua máquina virtual nas configurações, isso impede de malwares infectarem a sua rede local.

Ambiente de teste: Sandboxie

Neste momento, vamos aprender como executar programas específicos em uma "caixa de areia", isolada do computador utilizando o método Sandboxing. Para isso, iremos precisar de algum programa que cumpra esse dever, para esse guia utilizaremos o Sandboxie-Plus.

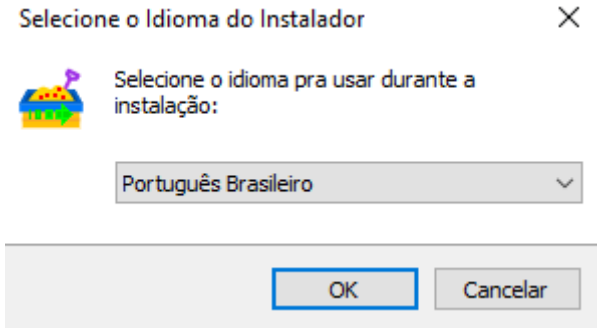
- Instalação: Para começarmos, vamos ao site de download oficial do Sandboxie-Plus e baixamos o arquivo de instalação.

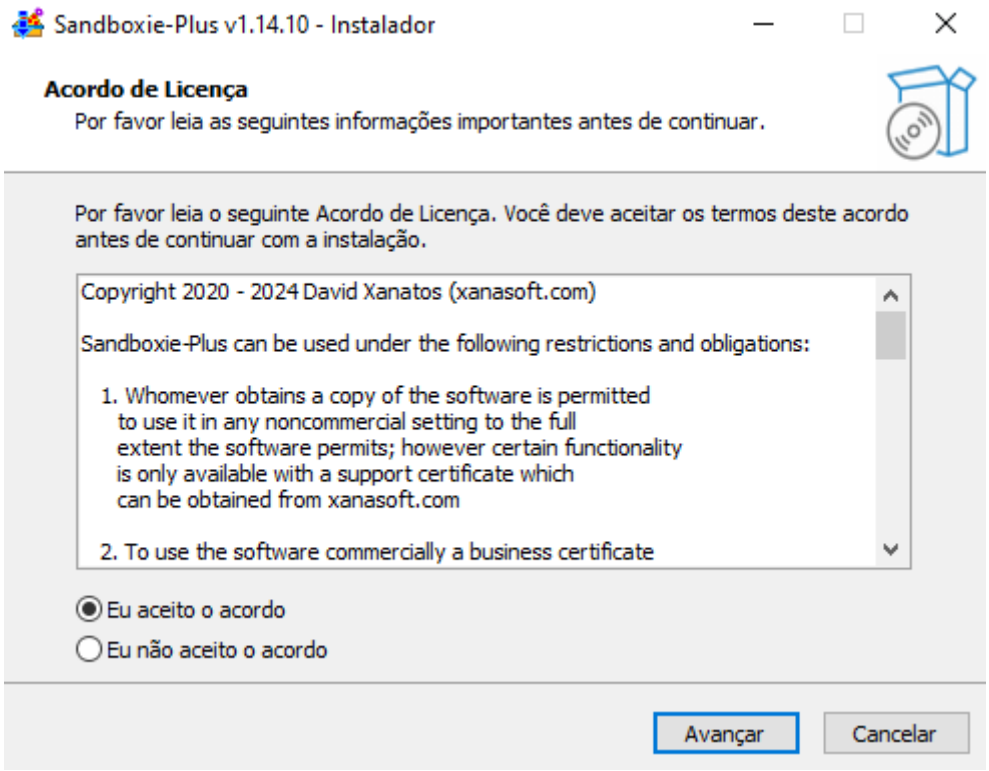
Selecione a última build de acordo com nosso sistema operacional

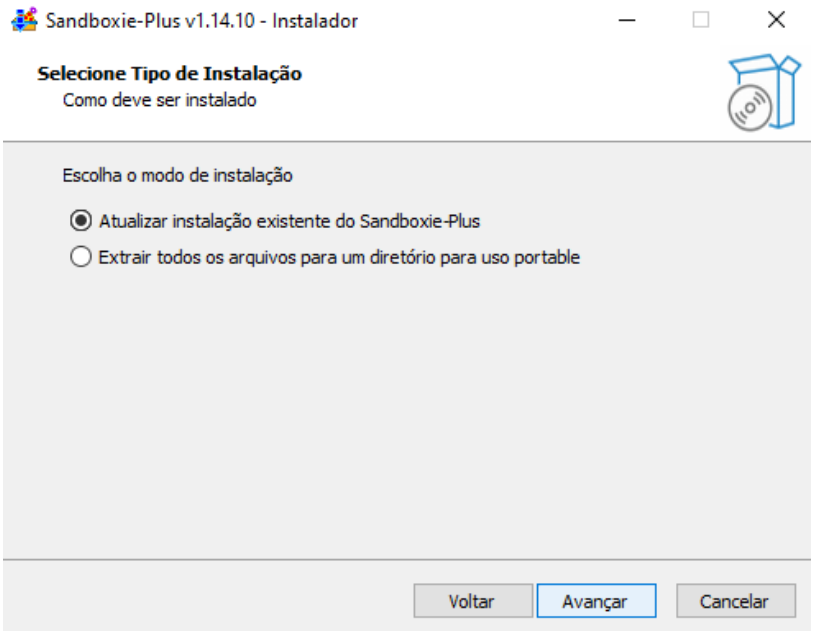


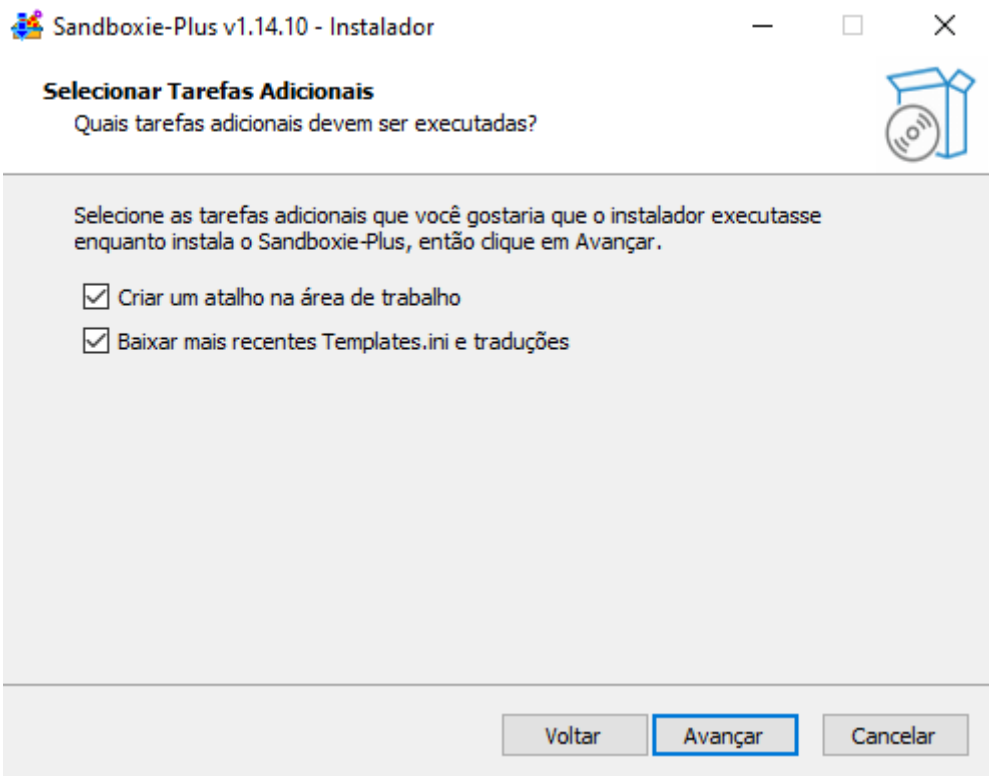
Execute o instalador na pasta em que foi baixado

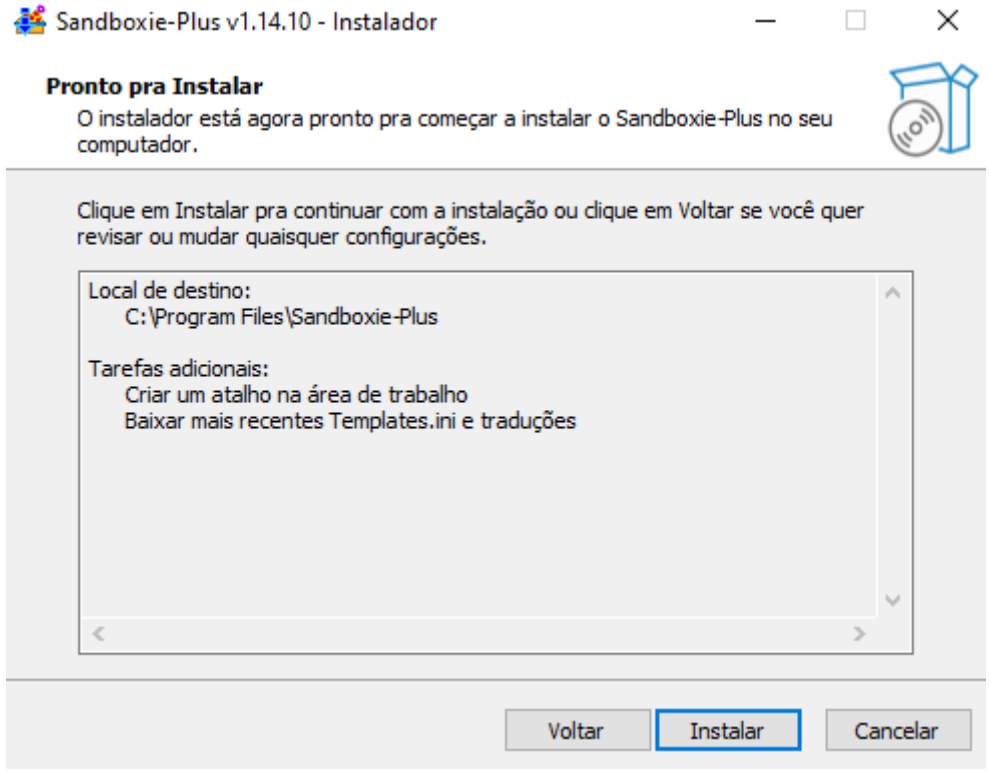
E aqui basicamente é só seguir a instalação normalmente como qualquer outro programa

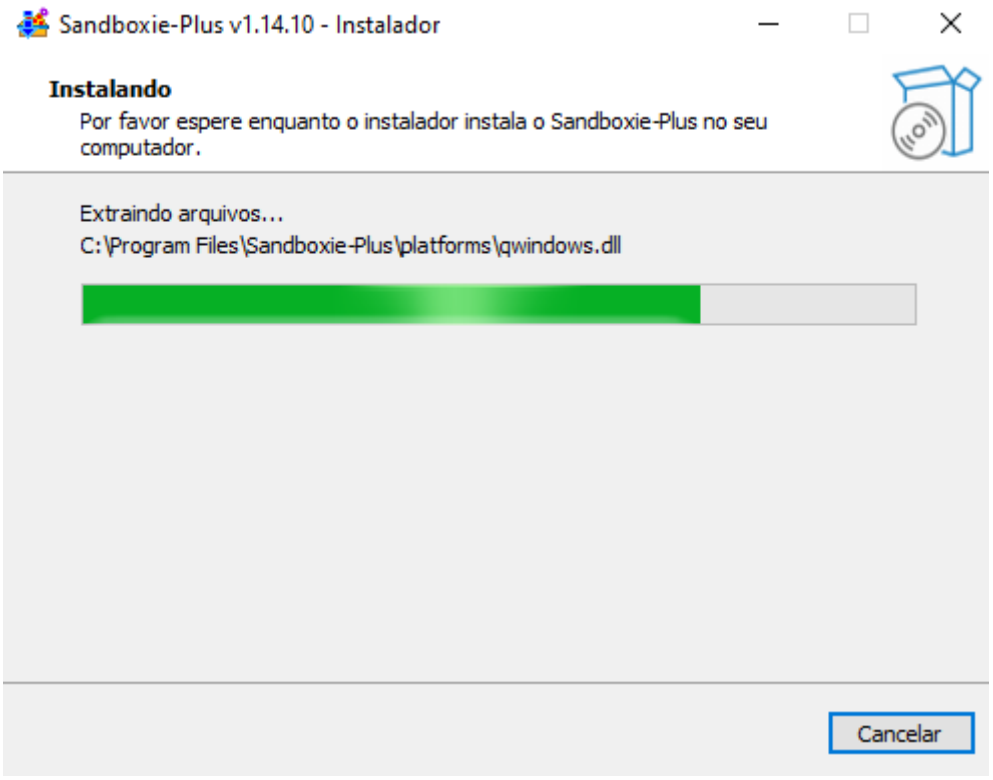


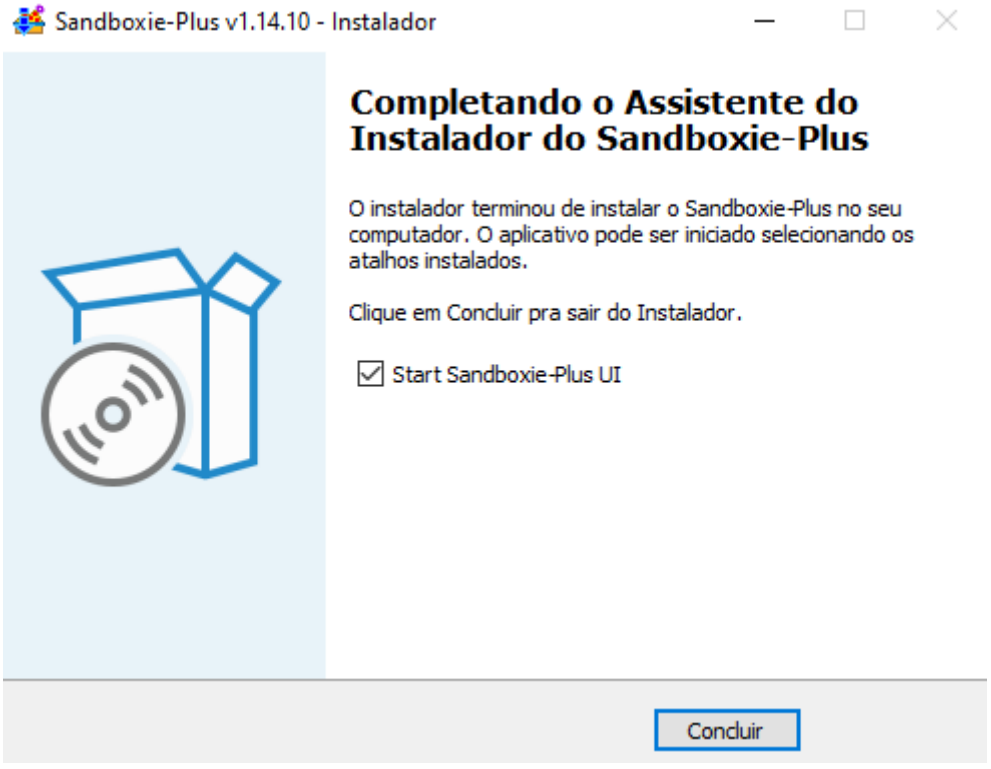





Sandboxie-Plus v1.14.10 - Instalador
Selecionar Tarefas Adicionais
Quais tarefas adicionais devem ser executadas?
Selecione as tarefas adicionais que você gostaria que o instalador executasse enquanto instala o Sandboxie-Plus, então clique em Avançar.
Criar um atalho na área de trabalho
Baixar mais recentes Templates.ini e traduções
Voltar
Avançar
Cancelar

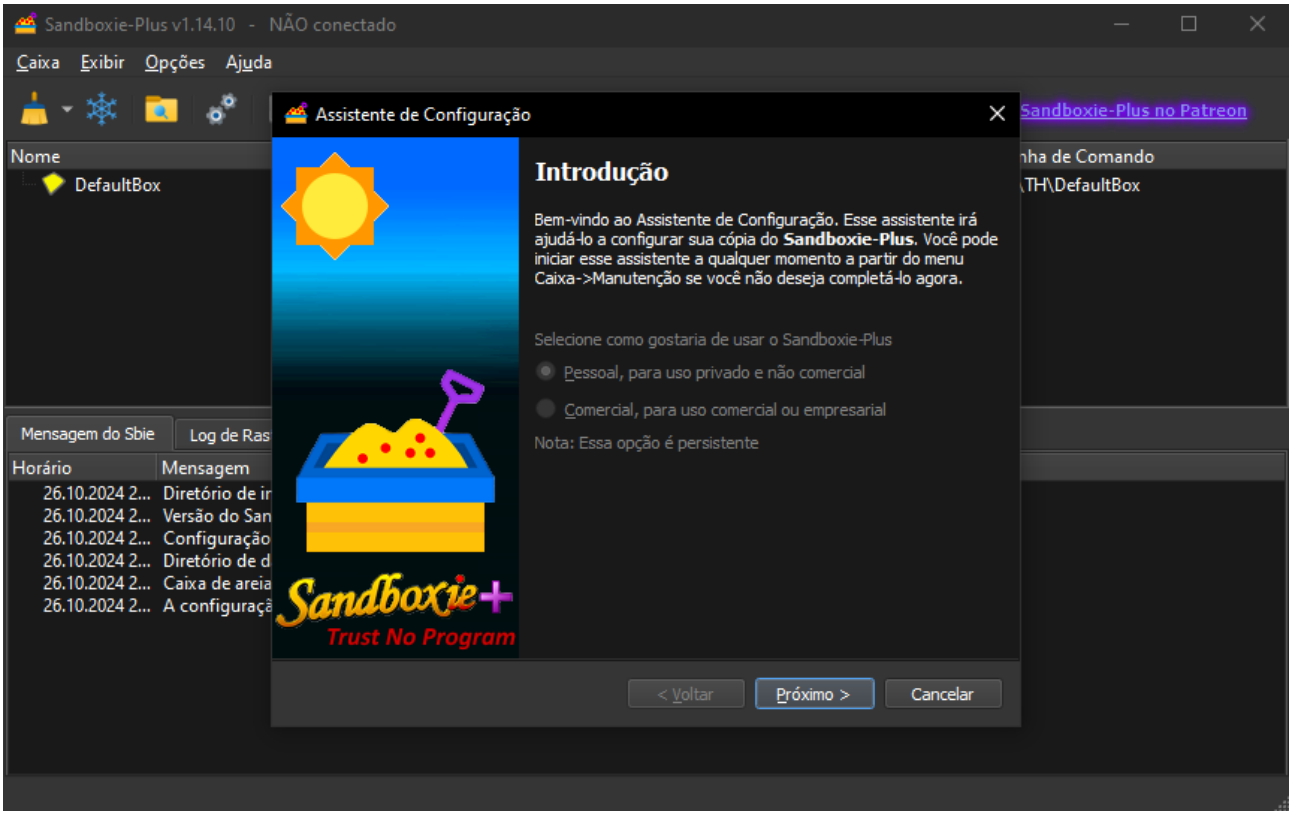

Sandboxie-Plus v1.14.10 - Instalador
Pronto pra Instalar
O instalador está agora pronto pra começar a instalar o Sandboxie-Plus no seu computador.
Clique em Instalar pra continuar com a instalação ou clique em Voltar se você quer revisar ou mudar quaisquer configurações.
Local de destino:
C:\Program Files\Sandboxie-Plus
Tarefas adicionais:
Criar um atalho na área de trabalho
Baixar mais recentes Templates.ini e traduções
Voltar
Instalar
Cancelar



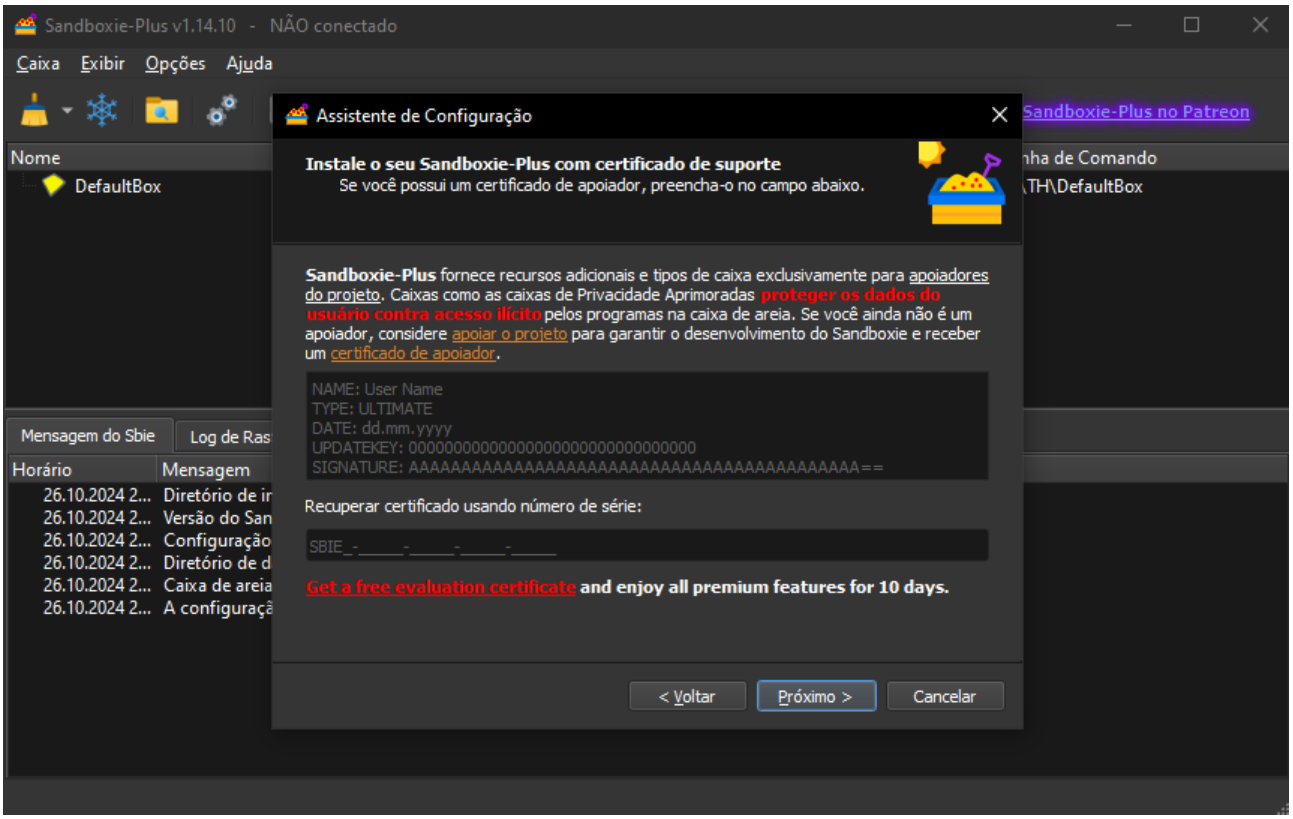


- Configurando o Sandboxie: Após instalar, execute o Sandboxie para que possamos configurar o programa

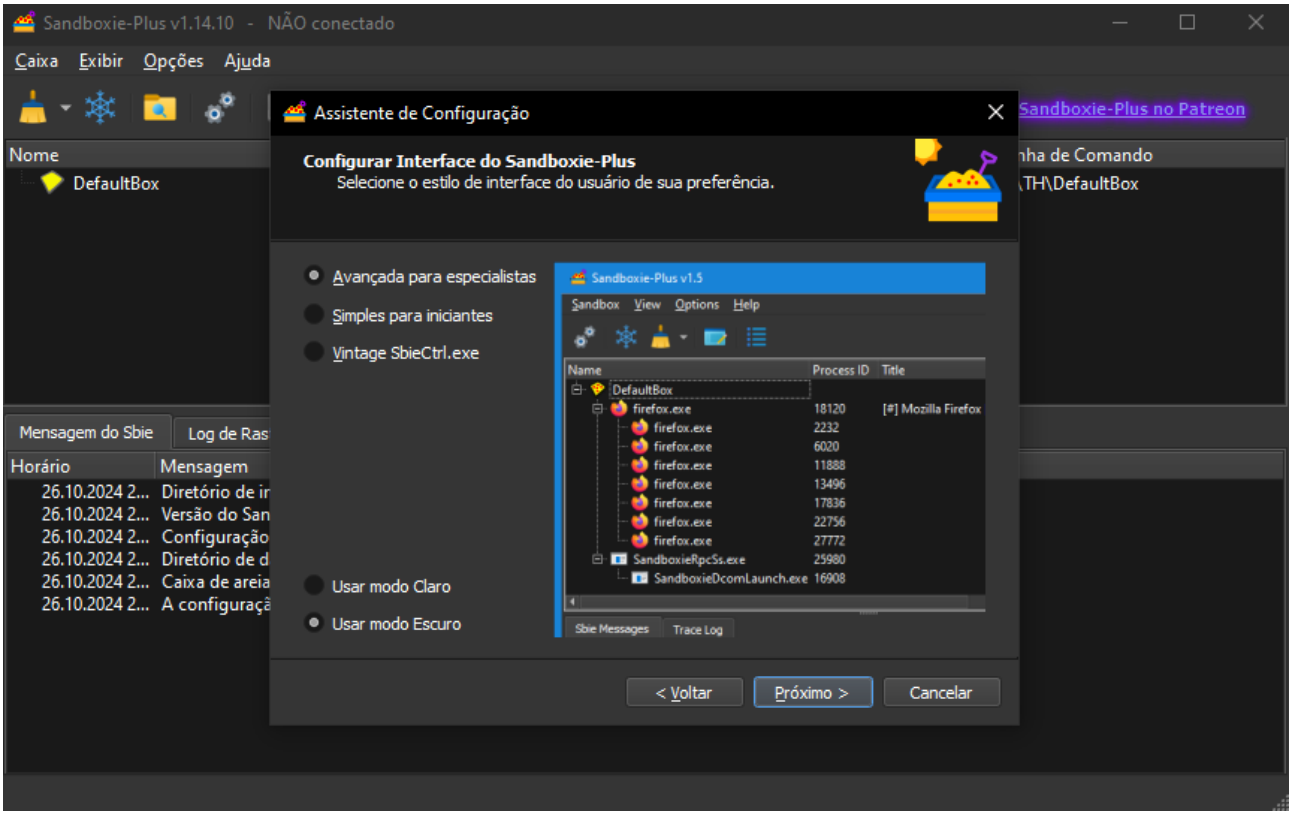
Nessa parte de tipos de uso, apenas aperte “Próximo”



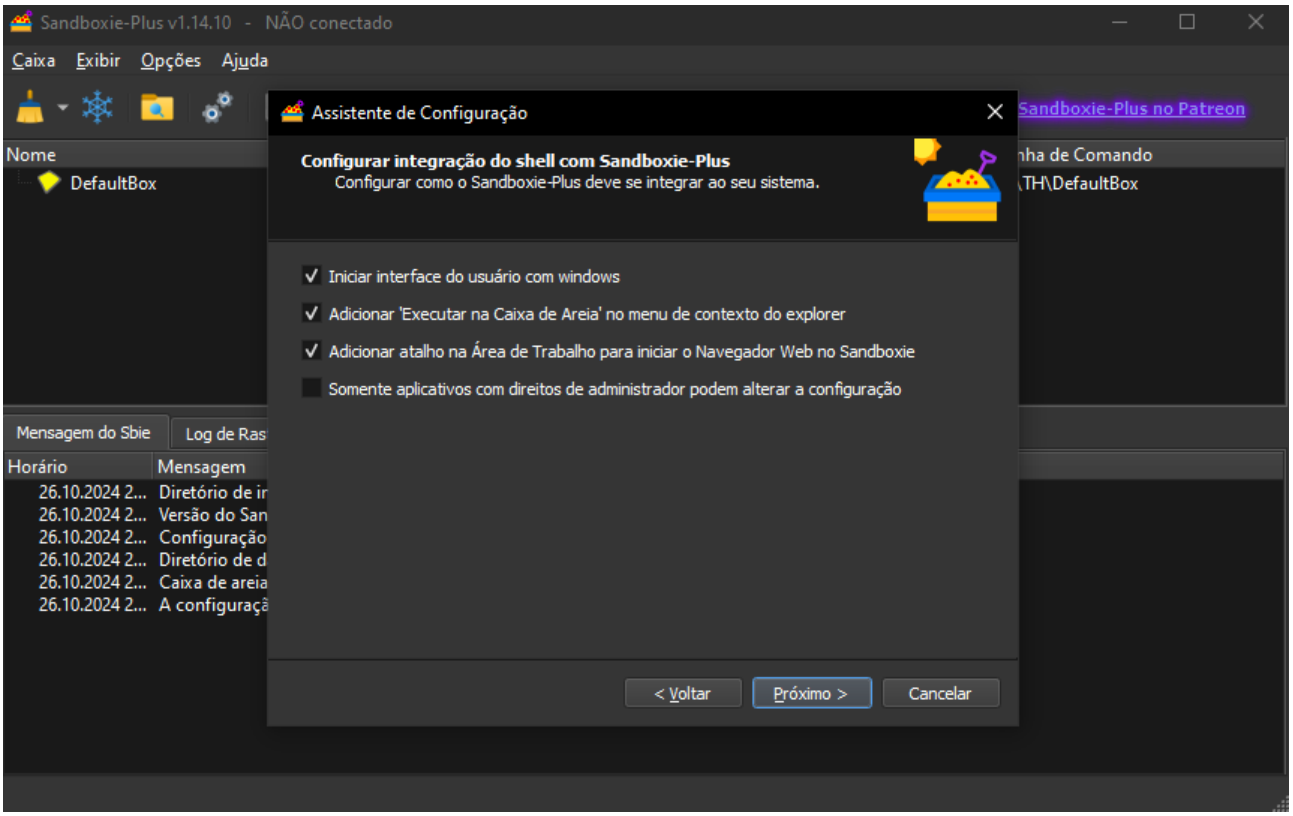
Aqui basicamente é uma forma de adicionar um certificado de apoiador aos desenvolvedores do projeto, como muito provavelmente você também não possui, apenas aperte “Próximo”



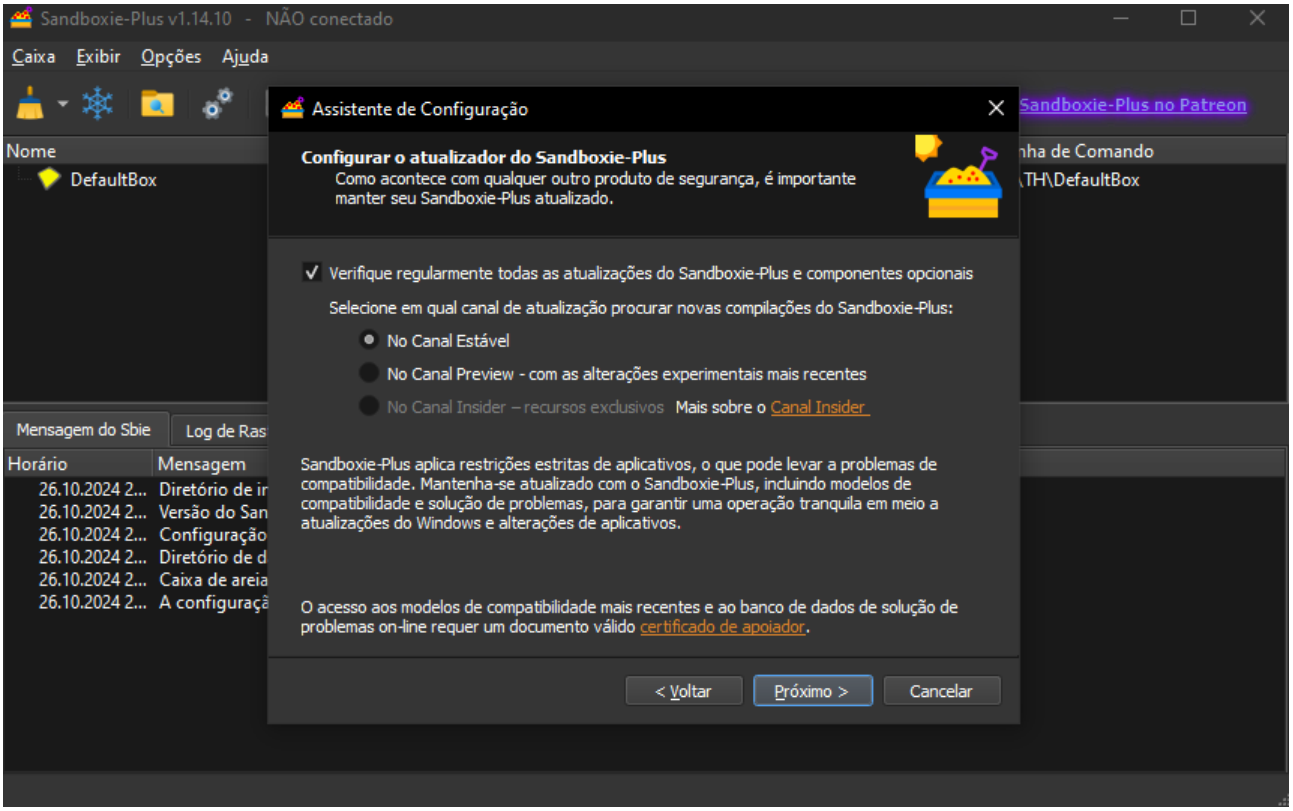
Nessa tela, certifique-se se marcar a opção “Avançada para especialistas”, para ter acesso a recursos mais avançados do programa, e o tema conforme sua preferência



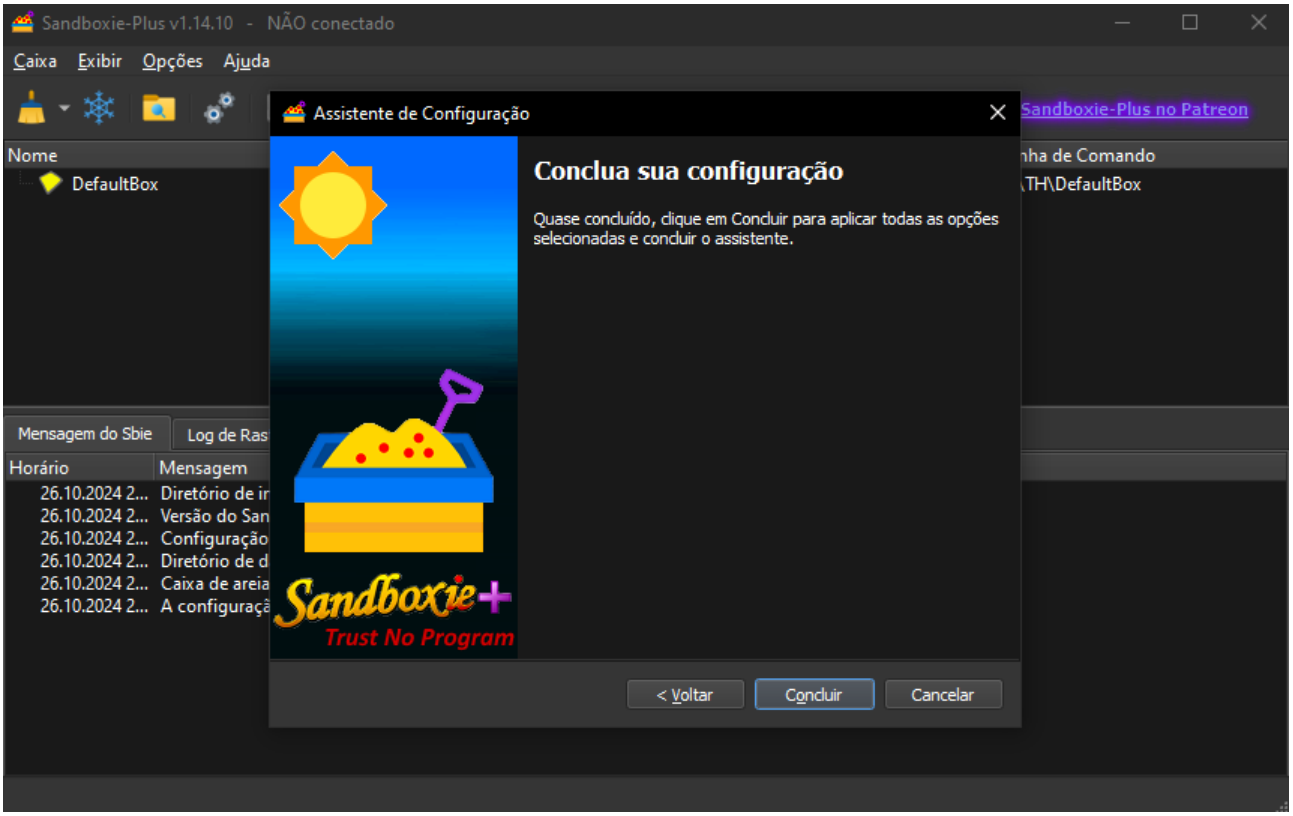
Só mude essas opções de acordo com sua preferência, caso contrário aperte em “Próximo”



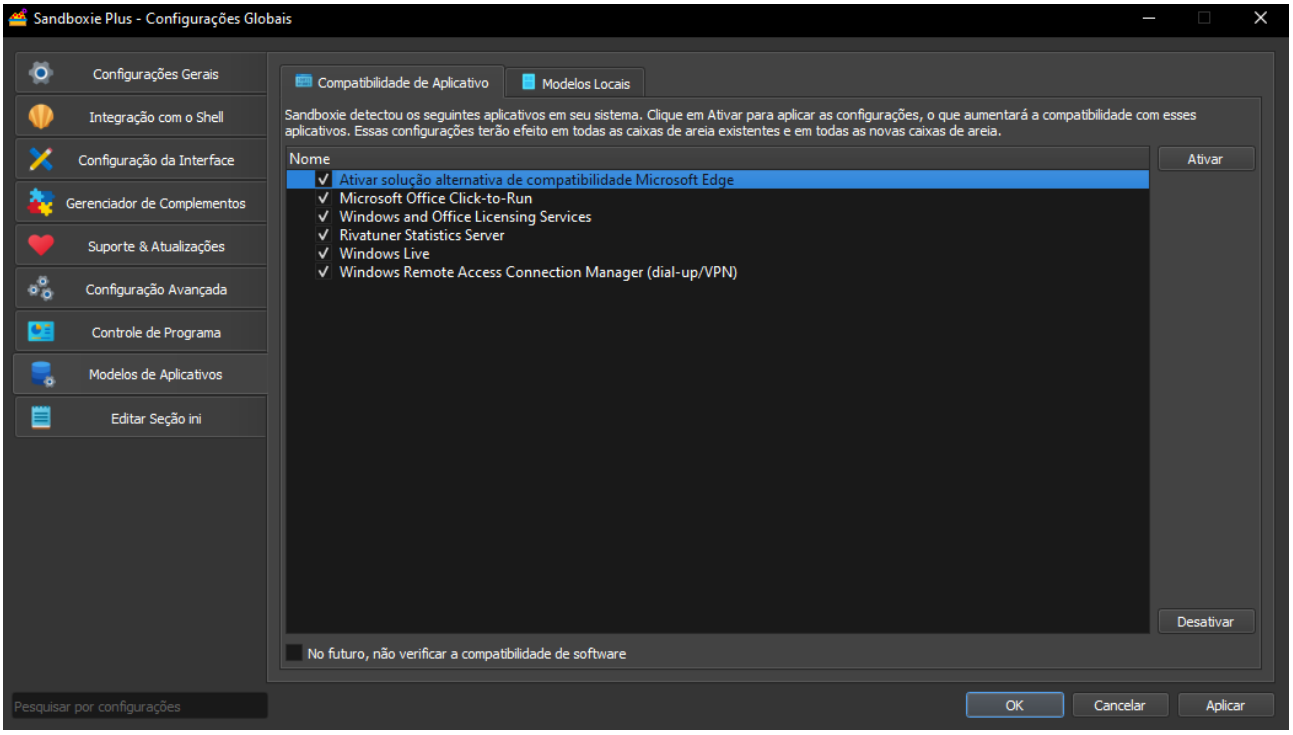
Nessa parte, é extremamente recomendado que você deixe marcado para buscar por atualizações do programa, isso garante uma maior segurança para programas executados nele



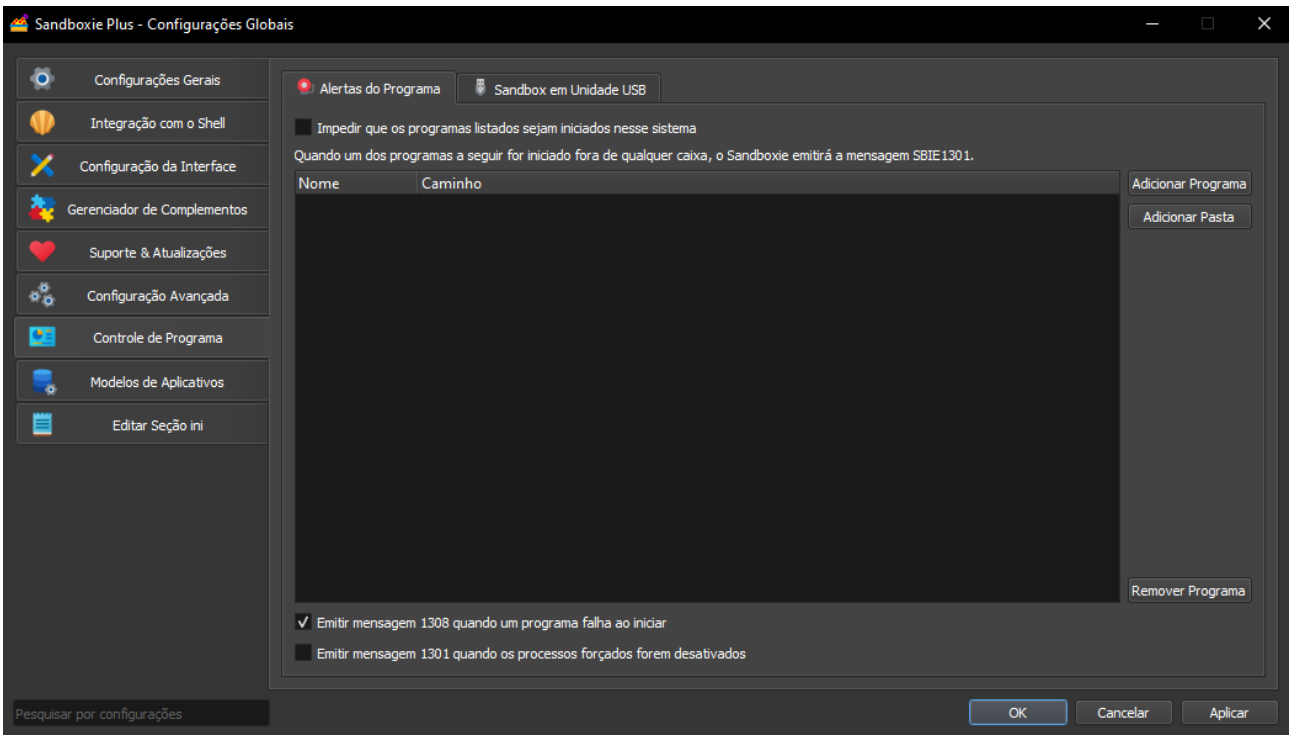
Conclua então suas configurações iniciais



É provável que suas configurações do programa tenham sido abertas automaticamente após concluir. Nessa tela, recomendo marcar todos os programas relacionados ao sistema para aumentar a sua compatibilidade com os mesmos

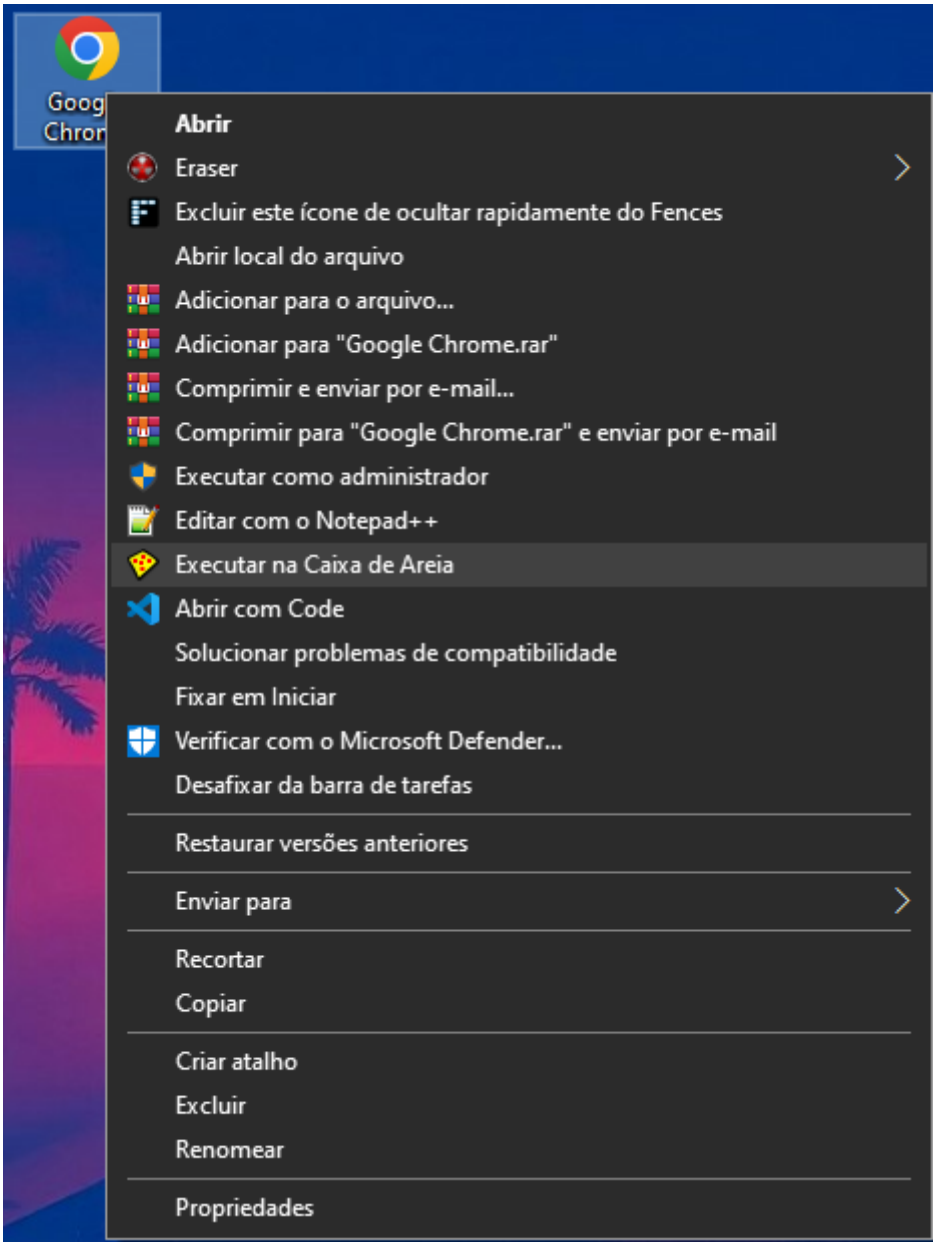


Na aba “Controle de Programa”, podemos listar todos os programas que nunca devem ser executados diretamente no computador, isso garante que o Sandboxie impeça dele executar fora da caixa de areia, tornando sua inicialização muito mais segura. Aplique as suas configurações e então estaremos prontos para começar a testar aplicações

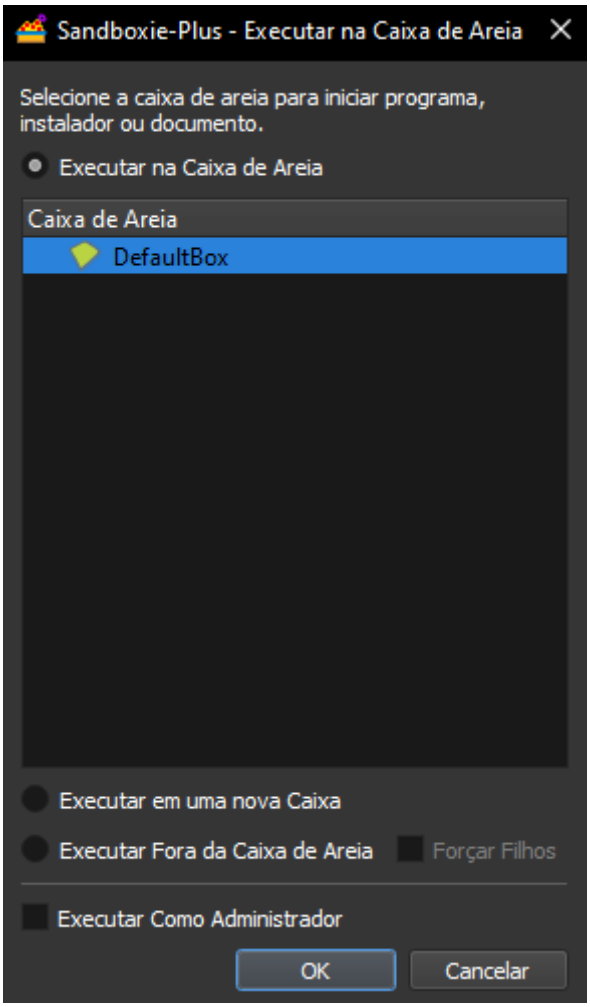


- Executando programas com segurança: Depois de configurado, iremos finalmente executar nossos programas em nossas caixas de areia.

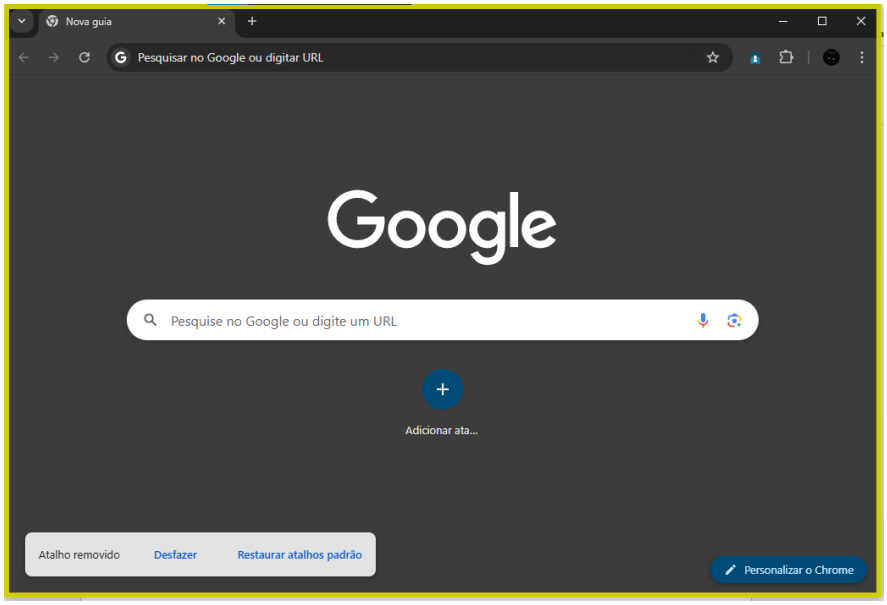
Por padrão, já é criada uma caixa de areia para executarmos nossos programas, utilizando dela, vamos executar um programa qualquer como exemplo. Para isso, escolha o executável do programa desejado, clique com botão direito e vá na opção “Executar na Caixa de Areia”



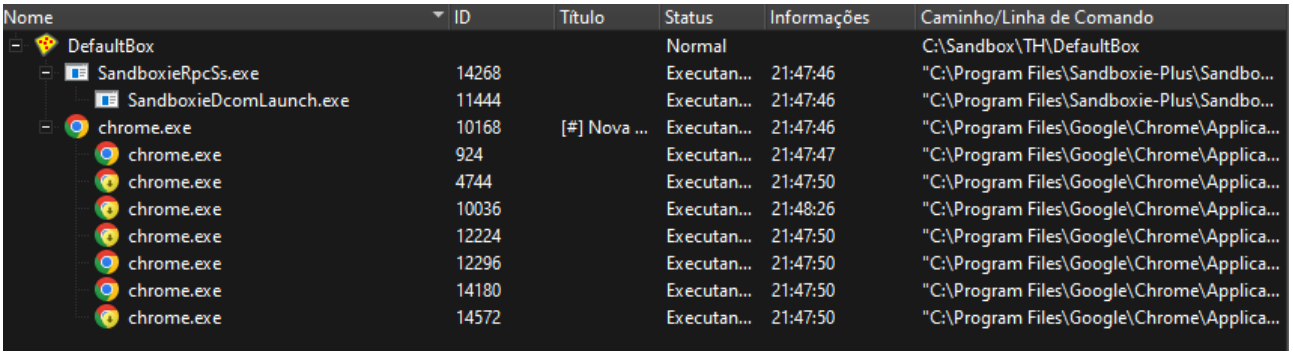
Uma guia do Sandboxie será aberta, então escolha executar em alguma caixa de areia existente, como a DefaultBox e aperte “Ok”

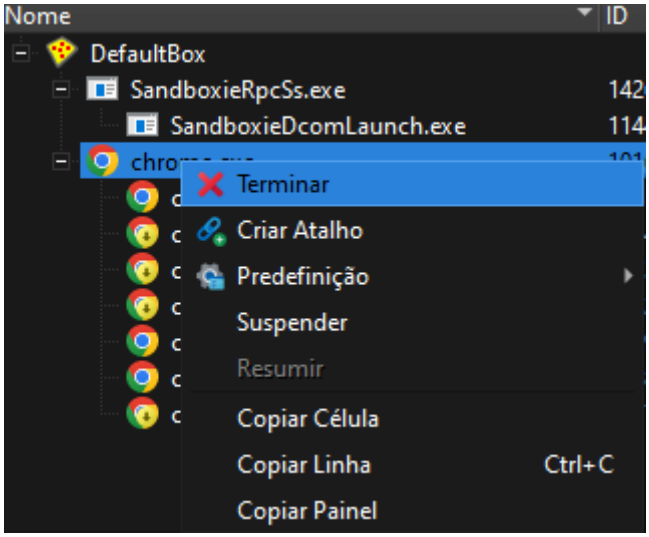


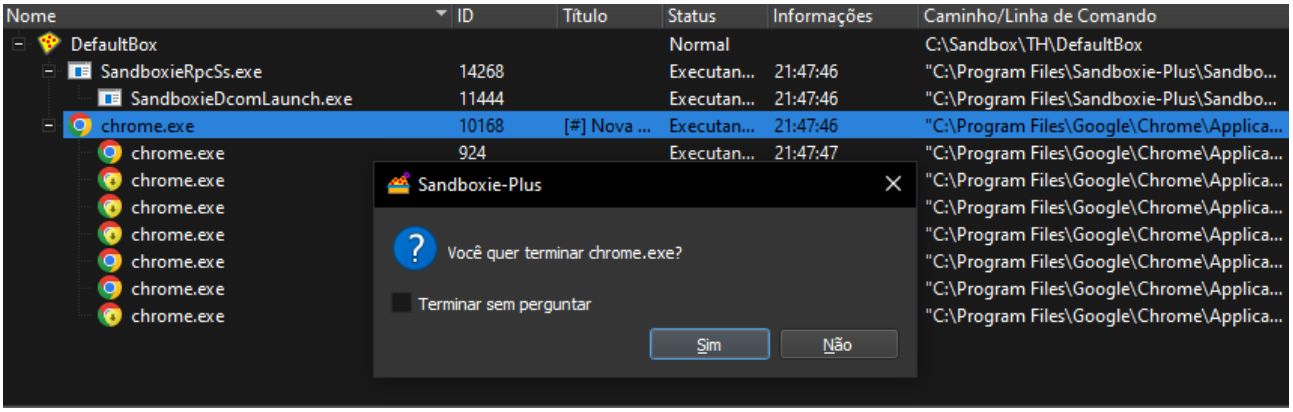
Dessa forma, o programa será aberto e ao posicionar o cursor na borda superior da janela, notará que a janela está circulada de amarelo, o que indica que ele está rodando em uma caixa de areia



Voltando ao Sandboxie, você poderá visualizar uma lista com todos os processos do programa que foi executado em questão, podendo dar task kill em algum deles, parecido com o gerenciador de tarefas, e até mesmo parar a execução na caixa de areia







Portanto, observa-se que executar programas em máquinas virtuais ou caixas de areia são formas extremamente interessantes de evitar malwares em seu computador.

Lembrando: Mesmo que seja seguro realizar execuções dessa forma, evite sair baixando coisas pela internet que são de fonte duvidosa, uma hora quem sabe essas ferramentas podem não funcionar como o esperado (o que é improvável), mas é mais recomendado.

Endereço de IP: Como Aumentar Sua Privacidade

Neste capítulo, vamos ver a definição de endereço de IP, sua importância, tipos de IP e principais motivos para camuflar um IP em determinadas circunstâncias.

O que é um endereço de IP?

O Endereço de Ip (Internet Protocol) é um identificador único destinado a cada dispositivo que está conectado à uma rede. Ele existe para identificar de onde surge um tráfego de dados solicitados ao provedor, que por sua vez pode identificar a localização de origem e demais informações contratuais vinculadas ao titular de um plano.

Por esse motivo, uma vez que alguém tem seu endereço de IP, fica extremamente fácil de te localizar geograficamente, rastrear informações pessoais de tráfego como histórico de navegação, direcionar ataques DDoS por meio de vulnerabilidades e, dependendo do caso (geralmente com ordem judicial), determinar quem é responsável pela contratação dos serviços com a operadora.

De forma geral, serviços que promovem a camuflagem de um endereço de IP possui diferentes regiões geográficas disponíveis para que o usuário possa se conectar do outro lado do mundo, isso possibilita o acesso a conteúdos que em teoria só seriam permitidos caso você habitasse o local dos mesmos, entretanto dessa forma é possível.

Dessa maneira, mostra-se bastante importante o direito de privacidade quando o assunto se trata de IPs, sendo bastante importante em determinadas situações mascará-lo para evitar possíveis invasores de realizar atos contra sua segurança.

Como camuflar meu endereço de IP?

Existem duas principais formas de ocultar seu enderço de IP: por meio de um proxy ou através de uma VPN.

- Proxy: Atua como um intermediário entre o dispositivo do usuário e a internet. Ao enviar uma solicitação de conexão, o proxy a redireciona ao site ou serviço final, ocultando o endereço IP original e apresentando o IP do servidor proxy.
- VPN: Cria um túnel criptografado entre o dispositivo e um servidor remoto, redirecionando todo o tráfego da internet através deste servidor. A VPN oculta o IP e, ao mesmo tempo, protege os dados transmitidos entre o dispositivo e o servidor.

Entretanto, por mais que seja recomendado ocultar seu IP de potenciais invasores na Internet, é extremamente recomendado que se utilize um serviços seguros de Proxies ou VPNs, como empresas confiáveis ou projetos open-source, a fim de evitar que empresas não-legítimas obtenham seu endereço de IP inconscientemente. Por isso, evite alternativas gratuitas que prestem esse tipo de serviço, caso encontre pesquise bastante para saber se de fato o programa encontrado é de uma fonte confiável.

Caso deseje realmente privacidade e anonimato, o mais ideal é assinar um serviço pago confiável e de qualidade que supra suas necessidades.

- Proxies e VPNs que recomendo:
  - ✓ NordVPN;
  - ✓ ExpressVPN;
  - ✓ ProtonVPN;
  - ✓ SoftEther VPN Gate;
  - ✓ Smart Proxy.

Exemplo prático: SoftEther VPN Gate

A fim de exemplificar como um serviço que mascara nosso endereço de IP real, vamos utilizar a VPN SoftEther, desenvolvida pela Universidade de Tsukuba no Japão, que basicamente como é um serviço gratuito, possui seus prós e contras.

A principal vantagem é a possibilidade de acessar conteúdos de forma anônima, possibilitando diversas conexões em regiões geográficas ao redor do mundo e mascarar o IP sem problemas relacionados a código malicioso, uma vez que o projeto é de código aberto.

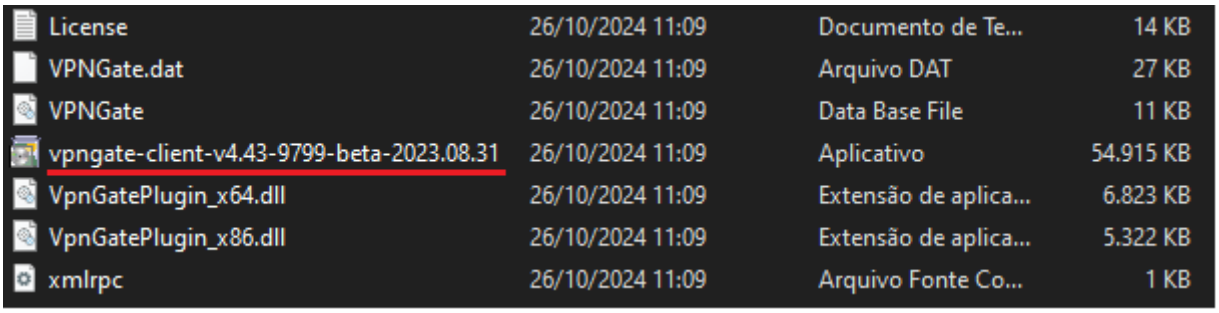
Entretanto, ela não é a mais indicada para atividades que requerem um grau extremamente elevado de sigilo, pois registra logs de conexão por até duas semanas após uma conexão, comprometendo um pouco o quesito “privacidade”.

De qualquer forma, estaremos utilizando ela pois supre nossas necessidades no momento e é inteiramente gratuita, sem assinaturas ou planos temporários!

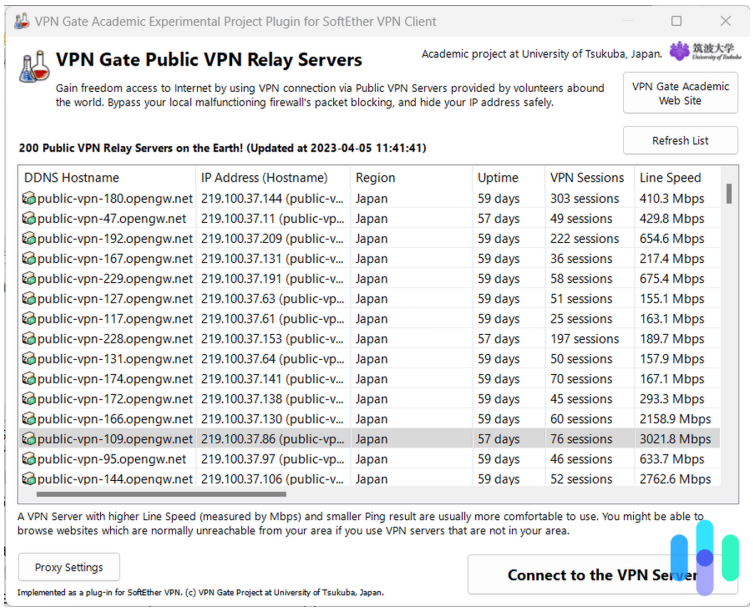
- Download da VPN: Para começarmos, vamos ao Site Oficial do Projeto para baixarmos o instalador.

Clicamos nesta opção em azul e então será baixado um arquivo zipado

Extraia o arquivo e abra o instalador a seguir



Após instalar, basta escolher uma localização para se conectar, dessa forma será alterado o número que identifica seu endereço de IP para o da localização escolhida.



Deep Web: Descentralização e Anonimato

A rede mundial de computadores, ou internet, possui uma vasta quantidade de conteúdos que são indexados por mecanismos de busca, como Google, Bing, Yahoo, etc. Porém, a verdade é que a maior parte dos conteúdos da internet estão indexados em outros mecanismos, que não podem ser acessados diretamente por uma simples pesquisa como os mencionados acima. Dessa maneira, surge a parte desconhecida da internet para muitos, a Deep Web.

Entendendo o conceito de Deep Web

Na verdade, essa parte da internet só é um pouco mais complexo de acessar por pessoas comuns, pois não envolve pesquisas comuns como fazemos em nossos navegadores convencionais. Para acessá-la, é necessário fazer uma pesquisa mais profunda sobre os conteúdos desejados, isso pode ser feito através de listas e diretórios de links disponíveis, como HiddenWiki e Harry 71.

No entanto, diferente do que o senso comum acredita e como ficou-se estigmatizado que a Deep Web é dividida em camadas, indicando o nível de dificuldade de acessar conteúdos de acordo com a sua camada atual ou representada como um iceberg que, conforme mais fundo você vai aprofundando, mais perturbadores e piores serão os conteúdos encontrados, na prática não funciona bem assim.

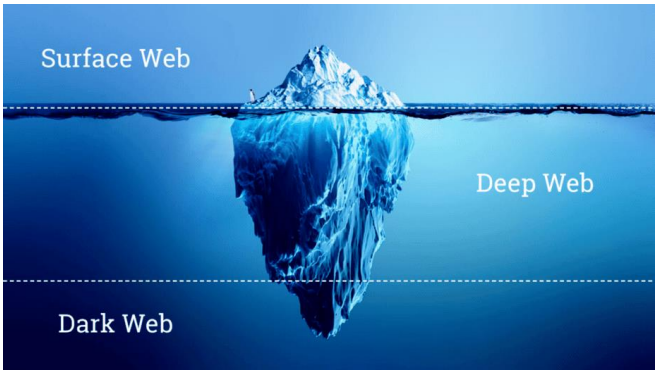
Na realidade, os conteúdos acessados serão considerados difíceis ou fáceis, perturbadores ou não de acordo com sua pesquisa e dedicação para fazê-la, não existe grau de dificuldade de acessar conteúdos, tudo irá depender da sua dedicação. Durante nossa navegação, deixamos de ser dependentes de um provedor de internet para solicitar acesso ao servidor de um site, por exemplo, sendo os próprios usuários dela os hosts das páginas, sendo chamada descentralização.

Por esses motivos, o termo “Dark Web” é considerado por muitos como sensacionalista, pois muitos influenciadores supostamente encontram conteúdos exclusivos que nunca foram vistos anteriormente na Deep Web, os quais são batizados como macabros ou sobrenaturais, sendo que na maioria dos casos aquele conteúdo foi simplesmente retirado de um filme ou obras fictícias. Aliás, é muito mais difícil encontrar conteúdos relacionados à crimes ou eventos sobrenaturais na Deep Web do que você imagina.

Lembre-se: A Deep Web por si só não é algo ruim. Muitas vezes, essa porção da Internet é utilizada por cidadãos de país que repudiam a liberdade de expressão através da censura e punições até mesmo severas, como prisão perpétua. Para contornar isso, eles a utilizam para se expressar abertamente sobre assuntos políticos ou religiosos, sem serem identificados. Sem contar com as inúmeras bibliotecas virtuais existentes lá, com uma vasta gama de conteúdos de utilidade pública.

Portanto, podemos concluir que os dois principais aspectos a serem tratados quando falamos de Deep Web são: **Descentralização e Anonimato**.

Discursos sensacionalistas sobre a Deep Web



Como acessar a Deep Web?

Para os interessados ou curiosos de plantão, vamos aprender nesse tópico a acessar a Deep Web de forma segura, evitando trackers/rastreadores e intrusos em nosso sistema.

Antes de tudo, é importante saber que somente acessar a Deep Web não irá infectar seu computador, muito menos alguém irá conseguir te rastrear (se fizer tudo da forma certa). O mais provável é você ser notado, de acordo com suas atividades lá, clicando em links, inserindo textos em forms etc, porém mesmo assim não saberão sua identidade real ou localização. Da mesma forma explicada antes, você só será afetado diretamente caso baixe algum arquivo malicioso de uma fonte suspeita ou insere dados pessoais em sites, mas se você apenas navega com moderação, sem sair clicando em tudo e, ainda por cima, utilizando destes métodos de segurança que serão apresentados, você muito provavelmente sairá anônimo na jogada.

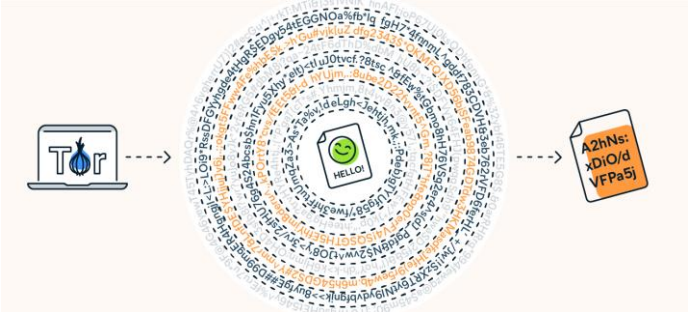
Antes de qualquer coisa, para garantir ainda mais nossa segurança, é extremamente recomendado utilizar uma VPN em nosso sistema real, para que mascare nosso IP real. Podemos utilizar qualquer uma que foi mencionada no capítulo anterior, isso além de proteger o sistema real como um todo, cria mais uma camada de segurança entre o sistema e a máquina virtual, evitando vazamentos de informações caso ainda sim você deixe alguma ponta solta para te rastrearem.

A melhor forma para acessar a Deep Web, de forma 100% anônima é utilizando virtualização, por meio de uma alguma máquina virtual e um sistema operacional que fornece serviços de anonimato e segurança específicos. Para virtualização, como estudado anteriormente, recomendo utilizar o VirtualBox ou VMware, já para sistema operacional, recomendo instalar o Tails ou Whonix, ambos fornecem um grau de privacidade e anonimato indiscutível, a diferença é que o Tails pode ser instalado em um pen-drive que é acessado simplesmente o inserindo na porta usb da sua máquina, sem uma instalação específica e a cada vez que desligamos o sistema, todos os dados são perdidos para sempre, sendo iniciada uma nova versão do mesmo.

Entretanto, podemos também acessá-la através do nosso próprio computador real, da mesma forma que acessaríamos pela máquina virtual, a única maior diferença é que estaremos correndo o risco de invasão de privacidade, pois o sistema é mais propício a isso, pois não possui recursos completos destinados a boas políticas de privacidade.

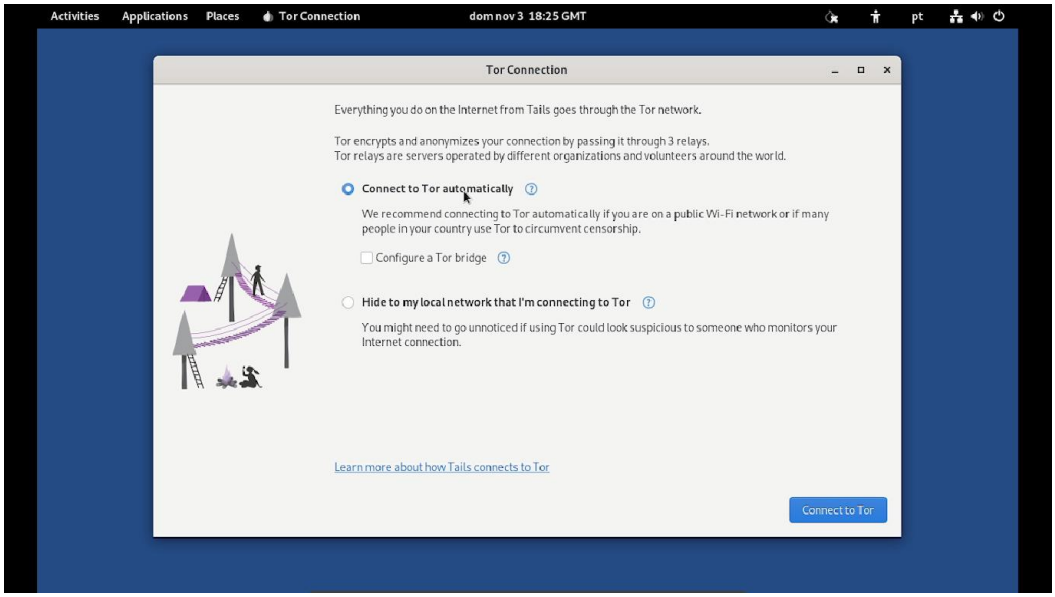
Vejamos o passo a passo a seguir, considerando que todos os requisitos anteriores foram seguidos:

- Escolhendo uma rede: Para iniciarmos, vamos escolher uma das redes que possibilita acessar links indexados pelos mecanismos de busca específicos dela. Temos diversas opções, sendo as principais Onion, I2P e FreeNet.
  Nesse material, estarei abordando a Onion, por ser uma das mais utilizadas e fáceis, além de ser inclusa nativamente no Tails, sistema operacional escolhido.
  Caso você escolha a Onion e outro sistema operacional, você pode instalar o navegador Tor, que fará a indexação de links .onion automaticamente.
  A rede Onion por si só apresenta um bom sistema de segurança e privacidade, uma vez que atua de forma de sobreposição de diversos endereços de IPs sobre o seu original, funcionando como camadas de uma cebola. Isso torna seu rastreio ainda mais difícil por parte de invasores ou rastradores. Por isso, se um hacker ou algo do tipo descobrir um endereço por trás do mascarado pelo Tor, ele cairá em outro endereço mascarado de outro lugar do mundo, e assim sucessivamente, até chegar no seu verdadeiro, o que é bastante difícil.



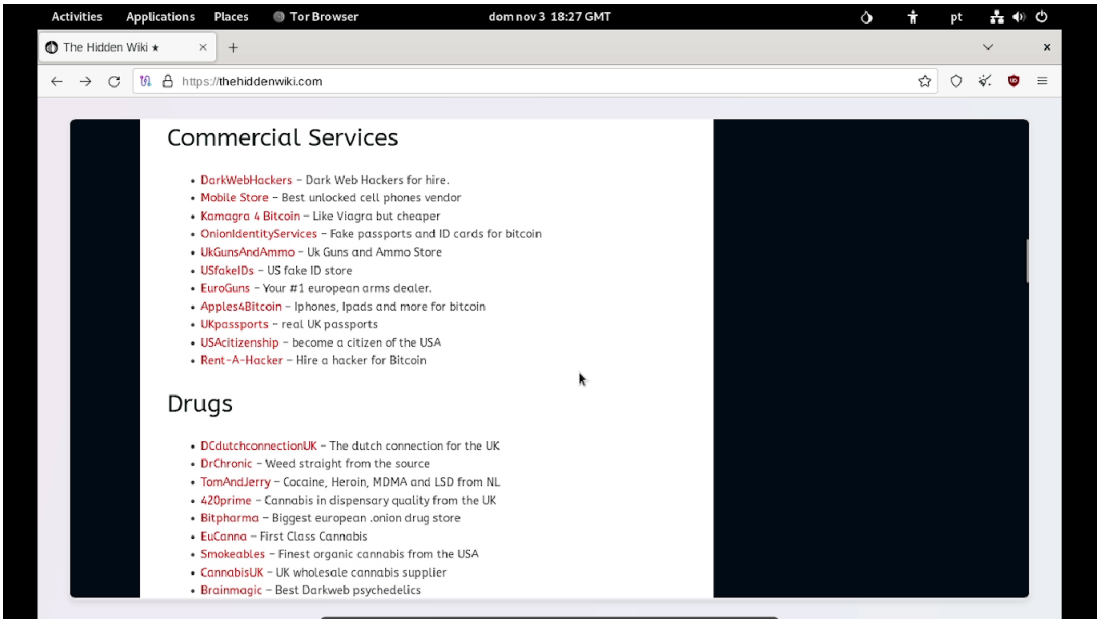
- Instalando o navegador: Cada rede mencionada possui seu próprio navegador que permite a indexação dos links referidos a ela, como o nosso caso foi a Onion, temos o navegador Tor para isso. No nosso caso, o próprio sistema operacional Tails possui o mesmo integrado nativamente. Mas caso queira instalar o Tor em outro sistema, como Whonix, basta ir no site oficial e realizar sua instalação.

Configuração nativa do Tor Browser no Tails OS



- Navegação: E a partir desse momento, se seguimos todos os passos anteriores, podemos iniciar nossa navegação na temida Deep Web, pesquisando links específicos em listas.

Minhas considerações: Seja cauteloso, saiba o que você está fazendo, não é porque você está anônimo que nunca será rastreado e acima de tudo: Não faça coisas erradas.



Criação, Complexidade e Gerenciamento de Senhas

Além de utilizar os métodos de segurança digital explicados nesse guia, uma das formas mais eficaz de garantir a segurança de contas, dados e informações pessoais sensíveis é por meio de senhas fortes. Isso inclui senhas de tamanho relativamente razoável, com diversas letras maiúsculas e minúsculas, números e caracteres especiais.

Todavia, também é preciso fazer o gerenciamento dessas senhas de forma segura e eficaz, para que nossas informações que, embora sejam senhas fortes, sejam vazadas e outras pessoas tenham acesso. Por isso, não é recomendado colocar todas suas senhas em um bloco de notas ou arquivo facilmente acessível em seu computador ou local físico, sendo mais importante esconder ao máximo essas informações para que apenas você tenha acesso a elas.

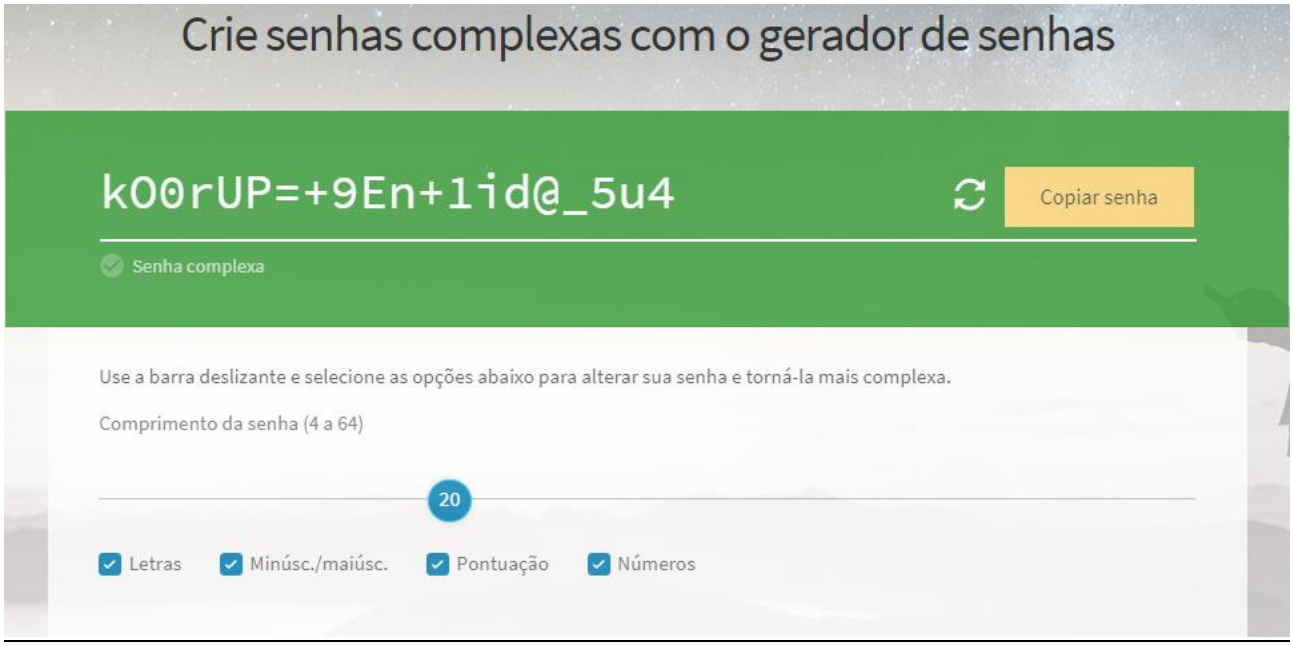
Por esses motivos, neste capítulo iremos aprender a criar senhas e gerenciá-las de duas maneiras: usando o Norton Password Generator e o KeePass.

Criando uma senha complexa

Há diversos serviços que permitem a criação de senhas seguras, para este guia escolhi o Norton Password Generator, por se tratar de um site que funciona em qualquer navegador

- Acessando o site: Para criarmos uma senha, vamos ao site oficial para isso.

Nessa parte, é tudo muito intuitivo, podemos inicialmente ver a senha que foi gerada, podendo copiá-la ou mandar o site criar outra. Além disso podemos ver a complexidade que a senha possui, entretanto veremos isso de uma forma melhor em outro site.



Nessa parte, podemos alterar o comprimento da senha, ou seja, o número de caracteres que ela possuirá e especificamos se queremos letras (minúsculas/maiúsculas), pontuação e números em nossas senhas.

A dica é sempre deixar o indicador de complexidade da senha no verde, prezando por uma maior segurança.

Verificando a complexidade de uma senha

A complexidade de uma senha é o que garante que a mesma seja forte ou não, tornando-a fácil ou difícil de ser adivinhada. Isso depende de alguns fatores que veremos a seguir, o que pode garantir que sua senha se torne mais complexa a partir de agora, evitando que invasores tentem de alguma forma acessar suas contas utilizando de tentativa e erro.

Senhas como "joao123" ou a data de nascimento de uma pessoa sempre foram muito arriscadas e previsíveis, entretanto muitos utilizam dessas por ingenuidade quanto ao risco que correm no meio digital, por esse motivo, o mais recomendado a se fazer é criar uma senha que seja extremamente forte e difícil de quebrar, sendo necessário muito tempo para adivinhá-la.

Geralmente, para se descobrir uma senha são utilizados os ataques de força bruta, feito através de tentativa e erro ao testar inúmeras possibilidades de senha em um determinado espaço de tempo.

Vejamos os cálculos para medir a complexidade e tempo para adivinhar uma senha:

- Complexidade: O cálculo de complexidade de uma senha é feito elevando a soma de caracteres possíveis dela pelo seu comprimento.

  Os tipos de caracteres são:

  - ✓ Letras minúsculas: 26 caracteres;
  - ✓ Letras maiúsculas: 26 caracteres;
  - ✓ Números: 10
  - ✓ Caracteres especiais: 33;

  Logo, o cálculo é feito da seguinte forma:

$$\frac{Caracteres\ possíveis}{Dígito\ 1} * \frac{Caracteres\ possíveis}{Dígito\ 2} * \ldots * \frac{Caracteres\ possíveis}{Dígito\ n} *$$

  Lembrando que o dígito de número n refere-se ao comprimento da senha em caracteres.

Ou seja:

$$Caracteres\ possíveis^{Comprimento}$$

Por exemplo, temos a senha DKALkdo%3#$320kkal, o cálculo de complexidade seria:

I) Identificando o comprimento da senha

$$Comprimento = 18\ caracteres$$

II) Calculando a soma dos tipos de caracteres que aparecem

$$Caracteres\ possíveis = 26\ + 26 + 10 + 33 = 95$$

III) Calculando a complexidade da senha

$$Complexidade = \ 95^{18} = 2.5 * 10^{35}\ combinações$$

- Tempo: Para calcular o tempo que alguém demoraria para descobrir sua senha, dividimos a complexidade da senha desejada pelo número de tentativas por segundo do invasor. Portanto, a fórmula fica da seguinte maneira:

$$Tempo = \frac{Complexidade}{Tentativas\ por\ segundo}$$

Utilizando nosso exemplo anterior, para 1 bilhão de tentativas por segundo teremos:

$$Tempo = \frac{2.5 * 10^{35}}{10^{9}} = 6.82 * 10^{18}\ anos$$

Ou seja, para nossa senha, o tempo que alguém levaria para descobri-la seria de aproximadamente 6,82 quintilhões de anos, na força bruta.

Gerenciando suas senhas

Aprendemos no tópico anterior a criar senhas mais fortes e impossíveis de quebrar, todavia, de nada adianta ter uma senha que cumpre esses requisitos sendo que você a armazena no bloco de notas no seu computador ou anota em um papel, guardado dentro de sua gaveta. Por esses motivos, o mais aconselhável é utilizar de um gerenciador de senhas seguro, para que só você tenha acesso à elas.

Existem diversas opções no mercado para gerenciar suas senhas, entretanto, fica um adendo

que preze pela sua segurança, ou seja, softwares que não possuem vulnerabilidades ou falhas na segurança e de preferência **código aberto**.

Minhas sugestões para esses serviços são:

- ✓ Bitwarden;
- ✓ KeePass;
- ✓ 1Password;

Apagando Arquivos Permanentemente do Computador

Neste capítulo iremos abordar uma ferramenta bastante útil em nosso dia a dia, o Eraser. Esse Software tem objetivo de apagar arquivos da memória não-volátil, ou seja, que estão armazenados permanentemente em seu HD ou SSD após desligar o PC. Veremos a seguir para que e como utilizar esse programa em sua máquina.

Por quê utilizar o Eraser?

Quando excluímos um arquivo pelo Windows e esvaziamos a lixeira imaginamos que estamos os apagando permanentemente, entretanto não é bem assim que a coisa funciona. Na verdade, após fazer isso, o seu disco rígido ou qualquer outro dispositivo de armazenamento que você utiliza deixa os dados desse arquivo ou programa sobrescritos em sua unidade, o que pode ser acessado mais tarde.

Por esses motivos surge o Eraser, uma ferramenta que após apagar o arquivo em questão, sobrescreve na unidade de armazenamento dados com padrões aleatórios e indecifráveis, tornando a recuperação dessa parte irreversível.

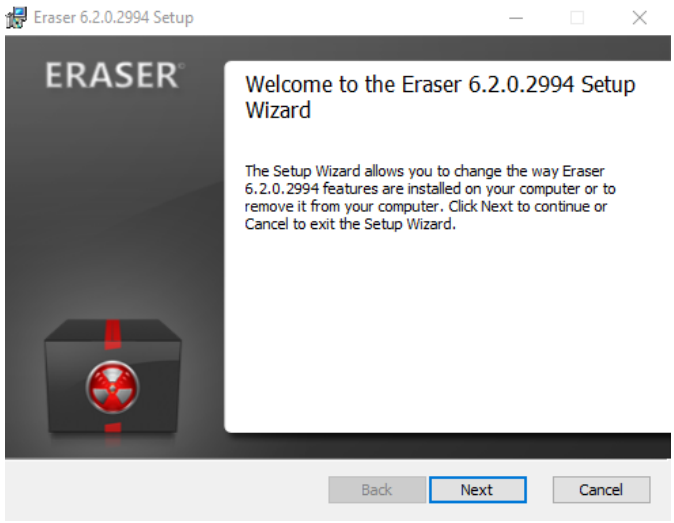
Dessa forma, ele é bastante útil quando desejamos apagar de fato arquivos que são muito importantes, como dados confidenciais e senhas.

Utilizando a ferramenta

- Instalação do Eraser: Assim como qualquer programa aqui apresentado, sua instalação é bastante simples. Basta ir ao Site Oficial do Programa e fazer o download do instalador.

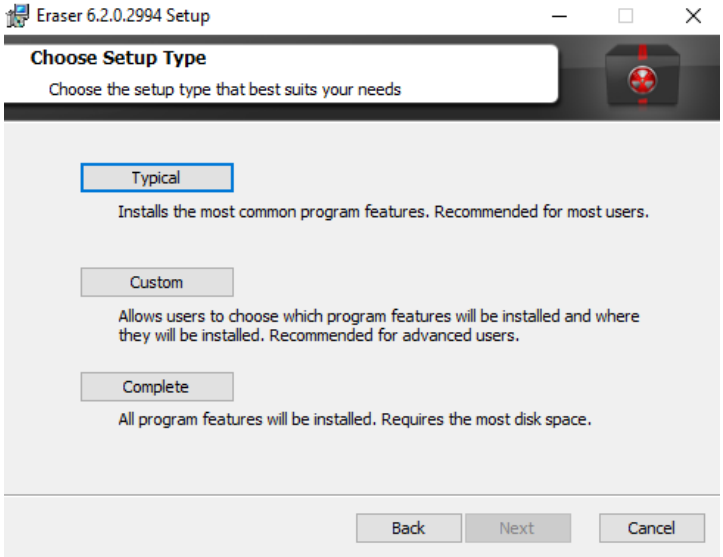
Execute o instalador que foi baixado

Basta ir clicando em “Next” para prosseguir na instalação

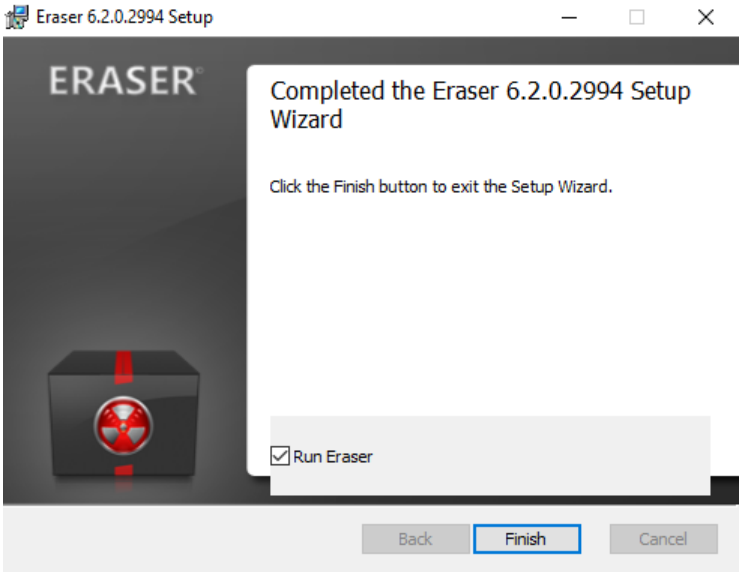


Aceite os termos de uso que ninguém nunca lê

Selecione “Typical” caso não venha por padrão e clique em “Install

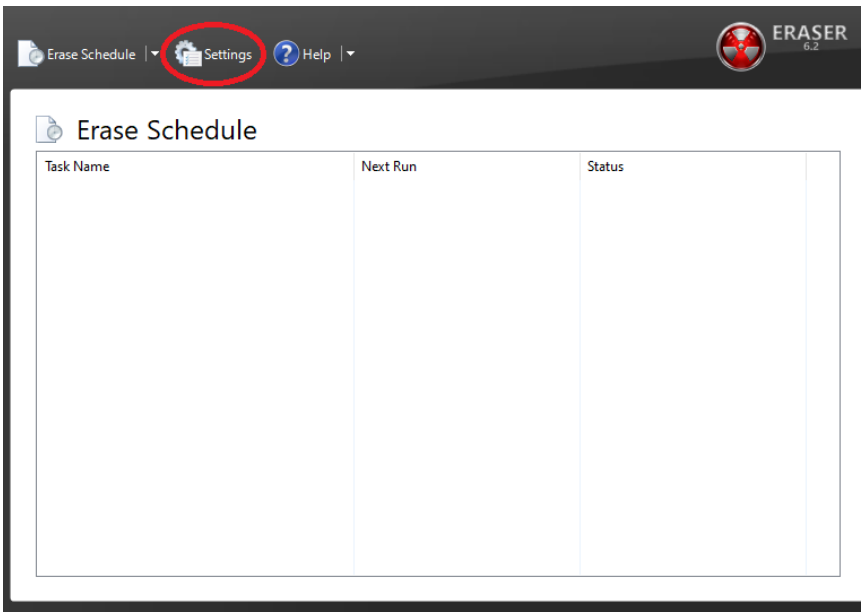


Após instalar, marque a opção para executar o programa após concluir

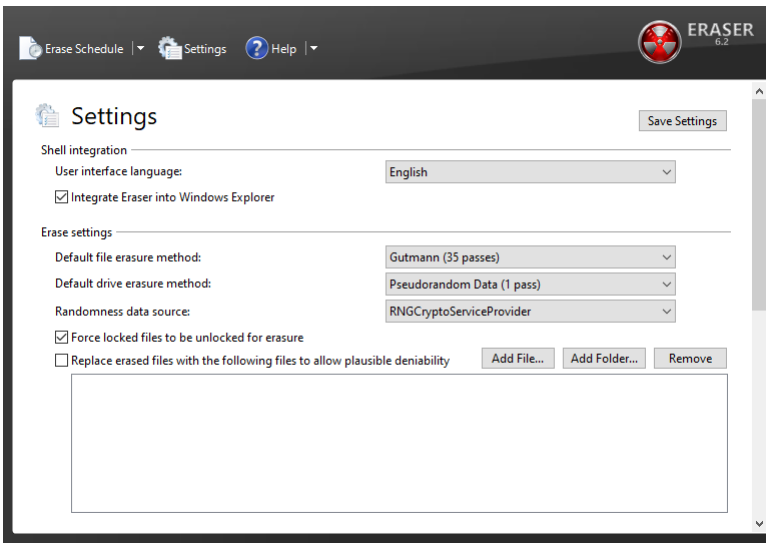


- Configurando o Eraser: Após executar o programa, vamos checar se as configurações estão corretas.

Clique na opção “Settings” para abrir a aba de configurações do programa

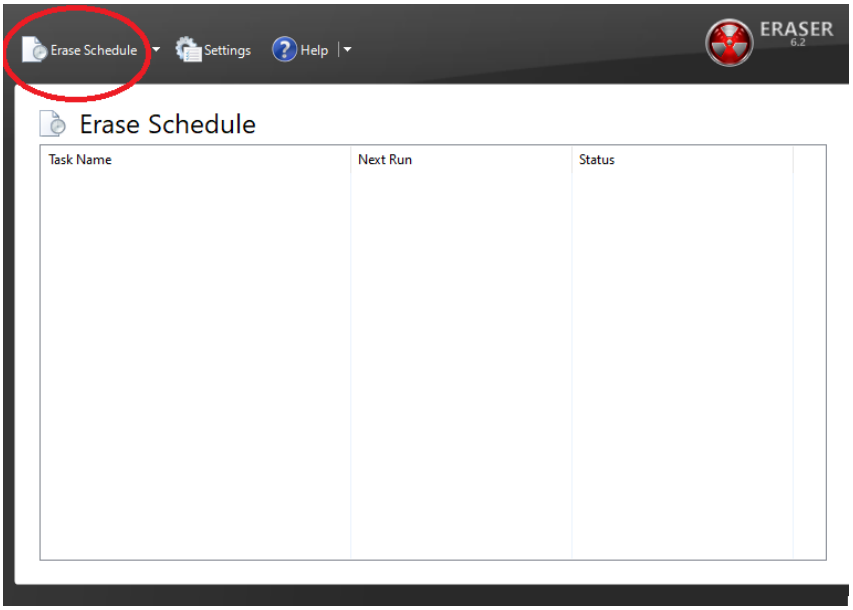


Nessa parte, você pode escolher o idioma de sua preferência. Mais abaixo temos configurações do modo de apagar arquivos, mas recomendo deixar o padrão caso não sabe do que as outras opções disponíveis alteram em sua funcionalidade.

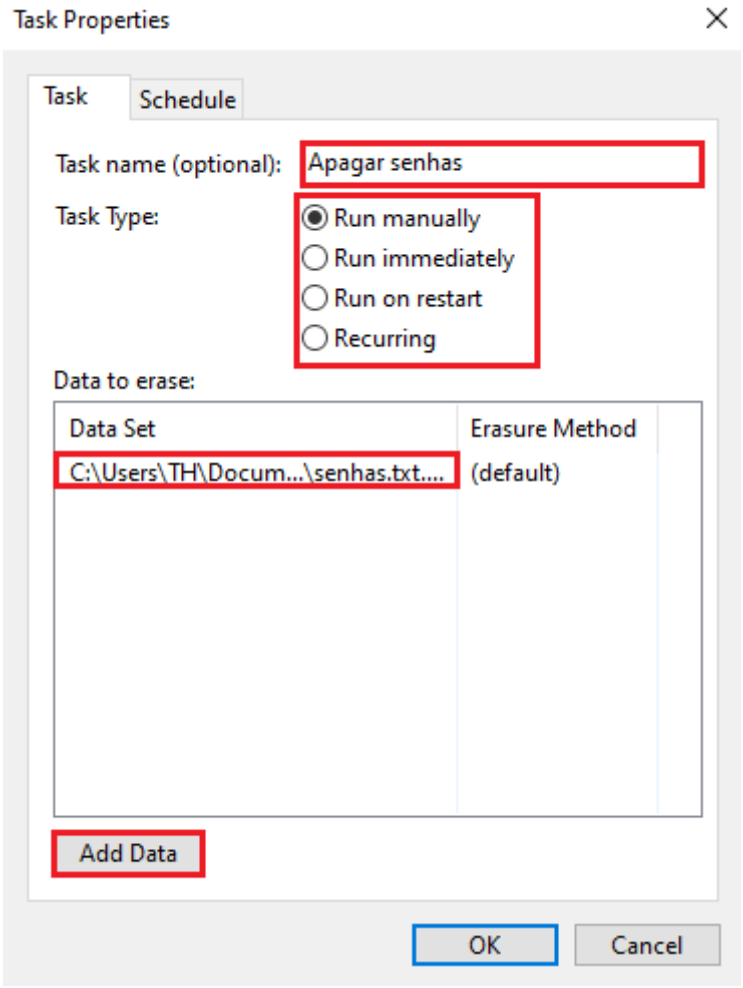


- Apagando os arquivos: Vamos agora aprender a apagar arquivos de duas maneiras: pelo próprio programa, imediatamente ou em algum determinado momento, e através da opção do sistema ao clicar com botão direito sobre o arquivo desejado.

Para apagar um arquivo pelo próprio programa, clique na opção “Erase Schedule”



Podemos renomear a nossa tarefa de exclusão no primeiro campo, escolher como essa ação será realizada marcando uma das quatro opções disponíveis.

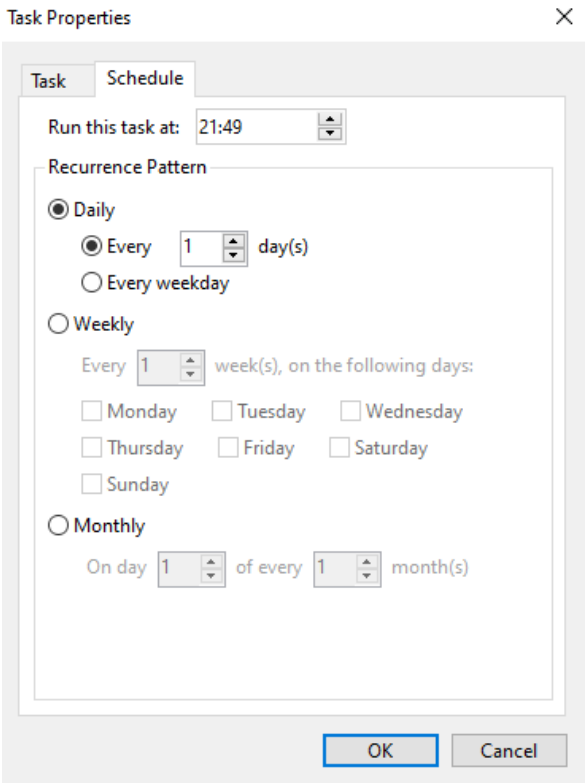


- Run manually: Você precisa apagar manualmente utilizando o eraser
- Run immediately: O arquivo é apagado imediatamente após a confirmação
- Run on restart: Após reiniciar o seu computador, o arquivo terá sido apagado
- Recurring: Você define um momento desejado para apagar o arquivo

Na aba “Data Set”, você pode ver todos os dados definidos para exclusão permanente, podendo editar os caminhos dos mesmos em disco rígido. Para adicionar um caminho de arquivo, basta clicar em “Add Data”

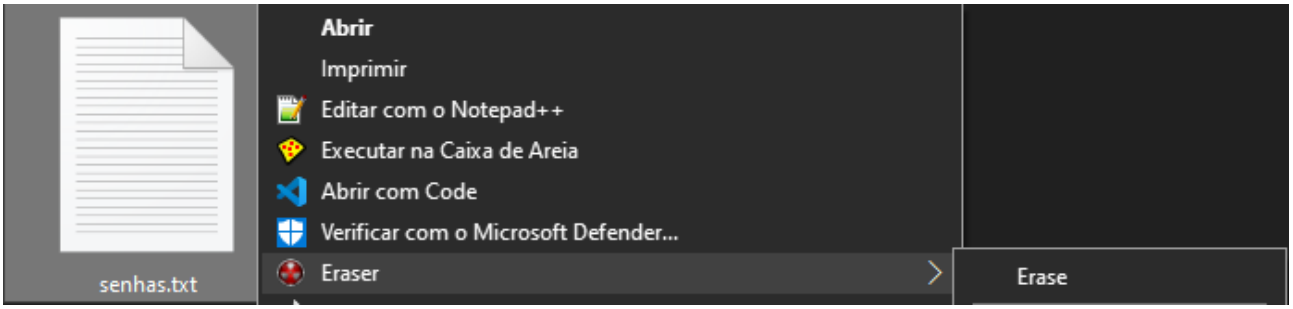
Obs: Para liberar a opção Schedule você deve estar com o tipo de tarefa em “Recurring”. Desse modo, é possível definir o horário que essa atividade será realizada em seu sistema e a frequência (diariamente, semanalmente etc). Isso pode ser bastante útil em diversas circunstâncias. Vamos supor que você esteja armazenando informações confidenciais periodicamente e queira que os arquivos sejam excluídos permanentemente nesse espaço de tempo,

isso pode tornar mais fácil essa ação e mais controlado.

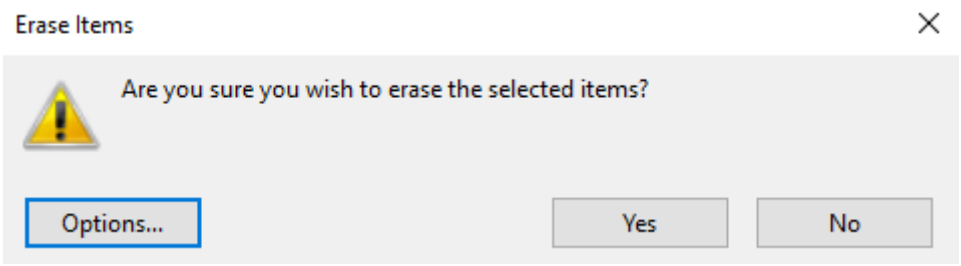


Após confirmar, todas suas exclusões serão realizadas de acordo com suas preferências definidas anteriormente.

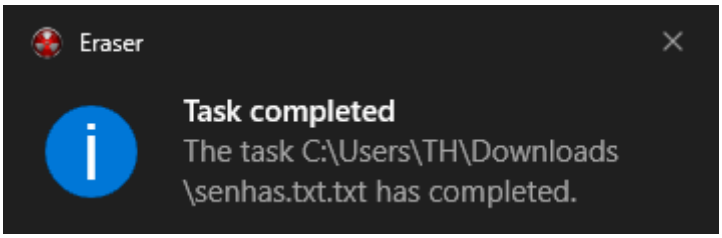
Outra forma de fazer todo esse processo mais diretamente é simplesmente indo ao arquivo que você deseja apagar permanentemente e clicando com o botão direito nele. Uma nova opção do seu sistema aparecerá, chamada “Eraser”.



Uma caixa de diálogo aparecerá para confirmar a exclusão



Caso tudo ocorra conforme o esperado, uma notificação irá aparecer indicando que o arquivo foi apagado com êxito



E dessa maneira aprendemos a apagar totalmente arquivos do nosso computador, caso prezemos ainda mais por uma segurança de dados confidenciais, por exemplo.

Conclusão e Agradecimentos

Dessa forma, terminamos o Guia Para Segurança Digital, agradeço imensamente a você que leu esse material até aqui, espero que de alguma forma tenha sido proveitoso e tenha absorvido alguma coisa, a fim de que mude sua postura e adquira novos hábitos de navegação.

Lembre-se: O verdadeiro antivírus é você próprio!

As minhas redes sociais podem ser acessadas por meio deste link a fim de tirar dúvidas ou simplesmente interagir conosco, seja muito bem-vindo (a)!