UNIVERSIDADE SAGRADO CORAÇÃO

DANIELLE RAMOS LÍBANO

UM ESTUDO DA DEEP WEB E ANÁLISE DE SUAS PRINCIPAIS VULNERABILIDADES

BAURU
2014

DANIELLE RAMOS LÍBANO

UM ESTUDO DA DEEP WEB E ANÁLISE DE SUAS PRINCIPAIS VULNERABILIDADES

Trabalho de conclusão de curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação, sob orientação do Prof. Dr. Elvio Gilberto da Silva.

BAURU
2014

Líbano, Danielle Ramos.

L694e

Um estudo da DEEP WEB e análise das suas principais vulnerabilidades / Danielle Ramos Libano. -- 2014.

68f. : il.

Orientador: Prof. Dr. Elvio Gilberto da Silva.

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade do Sagrado Coração – Bauru – SP.

1. DEEP WEB. 2. Anonimato. 3. Linux Tails. 4. TOR. I. Silva, Elvio Gilberto da. II. Título.

DANIELLE RAMOS LÍBANO

UM ESTUDO DA DEEP WEB E ANÁLISE DE SUAS PRINCIPAIS VULNERABILIDADES

Trabalho de conclusão de curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas da Universidade Sagrado Coração como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação sob orientação do Prof. Dr. Elvio Gilberto da Silva.

Banca examinadora:

_____
Prof. Dr. Elvio Gilberto da Silva
Universidade Sagrado Coração

_____
Prof. Me. Patrick Pedreira Silva
Universidade Sagrado Coração

_____
Prof. Me. Henrique Pachioni Martins
Universidade Sagrado Coração

Bauru, 08 de dezembro de 2014.

AGRADECIMENTOS

A minha família, pelo apoio e por cuidarem da minha filha para que eu pudesse estudar.

Aos meus amigos, por todos os estudos e trabalhos que realizamos juntos.

Ao Osmar, por me autorizar a estragar seu computador.

Aos meus professores, por lecionarem os conteúdos importantes para minha formação.

Ao meu orientador, pelo auxílio e tempo dispensados a mim.

A todos que estiveram presentes na minha jornada.

”Desliga isso e vem brincar comigo.”
(Marina Líbano)

RESUMO

A Deep Web vem crescendo cada vez mais, entretanto é utilizada de forma ilícita e desaprovada pela sociedade, o que causa muito preconceito e receio em ser utilizada por outras pessoas. Estar na Deep Web significa utilizar sistemas de navegação anônima, ou seja, proteger a identidade. Muitas pessoas não sabem que é possível utilizar a internet anonimamente, e mesmo se sabem, têm medo de utilizar tais recursos devido à fama de ataques e infecções por vírus aos que utilizam tal rede. Manter a identidade oculta na internet é importante quando se deseja manter a privacidade, e pessoas que correm riscos ao expressar certos assuntos a utilizam para se proteger, como por exemplo, os jornalistas e residentes de países que restringem a liberdade da informação. Com o intuito de orientar e esclarecer o assunto, este trabalho apresenta as características da Deep Web, as diferenças entre a mesma e a Web comum, e por fim, mostra quais são as configurações necessárias para se obter uma navegação segura. Para o desenvolvimento desta proposta foi montado um ambiente de ataque, foi criado um vírus do tipo trojan para infectar a máquina a ser invadida, para que se pudesse verificar em quais situações uma possível vítima fica vulnerável. Posteriormente foram configurados os ambientes a serem invadidos, ou seja, as configurações de antivírus e firewall foram alteradas, bem como foram utilizados sistemas operacionais diferentes e uma máquina virtual. As invasões foram elaboradas em 6 situações diferentes, o vírus foi enviado à suposta vítima com o firewall e com o antivírus ativos, com apenas um de cada ativo, e também com ambos desativados, ou seja, com a máquina completamente sem proteção. A vítima recebeu também o malware utilizando o Linux e posteriormente em uma máquina virtual.

Palavras-chave: Deep Web. Anonimato. Linux Tails. Tor.

ABSTRACT

Deep Web is growing increasingly, but it is used illicitly and disapproved by society, which causes a lot of prejudice and fear of being utilized by other people. Be on the Deep Web means utilize anonymous navigation systems, in other words, protect the identity. Many people are not aware that is possible to use the internet anonymously, e even if they know, they`re too scared to use such resources due to the fame of the attacks and infections by virus on those who use such network. Keep the identity hidden on the internet is important when one wishes to keep the privacy, and people who take risks when expressing certain matters use it to protect themselves, as for an example, the journalists and residents of countries that restrict the freedom of information. With the goal of orientation and enlightenment on the matter, this paper presents the characteristics of the Deep Web, the differences between this and the ordinary Web, and at last, show what the configurations necessary to obtain a safe navigation are. To the development of this proposition it was mounted an environment of attack, meaning, it was created a Trojan typed virus to infect the breached machine, to verify in what places a possible victim will be infected. Later it was configured the environments to be hacked, in other words, the antivirus configurations and firewall were altered, as well as been utilized different operational systems and a virtual machine. The breaches were elaborated in 6 different situations, the virus was sent to the supposed victim with the antivirus and firewall actives, with only one at a time actives, and also with both deactivated, which means, with the machine completely vulnerable. The victim also received the malware in a Linux and a virtual machine.

Keywords: Deep Web. Anonymity. Linux Tails. Tor

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ARPA	Advanced Research Projects Agency
CERN	European Laboratory for Particle Physics
DARPA	Defense Advanced Research Projects Agency
DOD	Departamento de Defesa
DNS	Domain Name System
EXE	Executável
HTTP	Hyper Text Transfer Protocol
IIP	Invisible Projeto Internet
I2P	Invisible Internet Project
IP	Internet Protocol
MIT	Massachusetts Institute of Technology
NetDB	Network Database
NRL	Naval Research Laboratory
SO	Sistema Operacional
ONR	Office of Naval Research
P2P	Peer-to-peer
RAM	Random Access Memory
TCP/IP	Transmission Control Protocol/Internet Protocol
TOR	The Onion Router
URL	Uniform Resource Locator

SUMÁRIO

1 INTRODUÇÃO

A Internet foi criada com a finalidade de compartilhar e proteger informações militares no auge da Guerra Fria. Para tanto foi desenvolvida uma ligação entre computadores para que fossem feitas transmissões de informações militares, e com o passar do tempo, tal conceito, embora com fins acadêmicos, foi expandido para universidades norte-americanas. (WETHERALL; TANEMBAUM, 2011).

No início dos anos 90 a Internet que hoje conhecemos como Web começou a se popularizar e era acessada até então por pesquisadores, cientistas e hackers[1]. Os sites não tinham uma aparência agradável e o acesso era complicado, sendo feito por linhas de códigos muito específicos.

A popularização da Internet se deu quando um jovem chamado Marc Andreessen idealizou um mundo onde todos os computadores, e todas as pessoas teriam acesso a mesma, pois ele a considerava algo muito útil e inovador.

Marc e seus amigos formaram um grupo e desenvolveram um navegador chamado Mosaic Online que foi lançado no ano de 1993, o qual foi o precursor dos navegadores que utilizamos hoje. O que eles fizeram foi deixar a navegação mais simples e intuitiva, utilizando arquivos de imagem, vídeo e som, o que deu início à popularização da World Wide Web. (A GUERRA..., 2008).

Hoje a Internet é utilizada para quase tudo no dia a dia das pessoas, mas existe uma reclamação frequente da falta de privacidade na Web, onde constantemente os dados pessoais dos usuários que deveriam ser privados acabam sendo divulgados. Empresas como Google e Facebook mantém um registro de tudo o que as pessoas fazem e já fizeram, pois tudo é armazenado, e isso é considerado pelos internautas uma forma de vigia, e as pessoas não gostam de ser vigiadas.

Com a popularização da Internet e o acesso facilitado, surgiu a necessidade de segurança da informação, sendo criada uma rede diferente de compartilhamento de arquivos conhecida principalmente como Deep Web.

Nesta arquitetura de rede seus sites não são localizados por buscadores comuns como o Google, por exemplo, e toda sua navegação é anônima e criptografada. Isto ocorre pelo motivo do usuário permanecer oculto, então as

[1] Indivíduo que se dedica a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores. (OLIVEIRA, 2003).

pessoas que dão valor à privacidade optam por usar tal rede. (SYVERSON, [2005?], tradução nossa).

Como os usuários não podem ser localizados ou identificados, as pessoas aproveitam o benefício do anonimato para divulgar e distribuir materiais considerados ilícitos e criminosos de acordo com as leis vigentes nas Constituições Federais de vários países. Tais materiais podem ser encontrados em forma de imagens ou vídeos com cenas de violência como estupros, assassinatos, tortura de animais ou de pessoas, experimentos científicos com humanos, pedofilia, entre várias outras ações de natureza hedionda.

O comércio é vigente nessa rede, também conhecida como Dark Net. Utilizando o Bit Coin, uma moeda virtual, e também criptografada para impossibilitar o rastreamento do comprador e do vendedor, é possível comprar drogas, armas, remédios, encomendar assassinatos e até mesmo órgãos. Entre uma vasta gama de coisas consideradas bizarras, existe ainda o canibalismo, e até tutoriais ensinando como preparar a carne humana.

Devido ao grande número de coisas ruins que circulam por esse submundo, existe muito receio entre as pessoas em se aventurar por lá, mas ainda assim, pode-se usar de maneira muito boa e proveitosa tal recurso. É possível encontrar livros, filmes e músicas raras que não estão na Web, bem como tutoriais, e discussões em várias áreas de conhecimento. Existe muito conteúdo que não pode ser encontrado na Web convencional porque a mesma é vigiada e monitorada, o que não acontece na Deep Web.

Em países em que a Internet é vigiada e vários sites são bloqueados, as pessoas podem encontrar libertação de tal censura utilizando o anonimato da rede profunda.

Hackers também utilizam a Deep Web para testar softwares e vírus, por isso é necessário cautela para garantir uma navegação segura. Existem grupos de hackers no mundo inteiro, chamados de Anonymous, os quais se juntam para tentar derrubar sites e sistemas, e o encontro acontece em data e hora marcada em algum lugar da rede oculta.

Para acessar a Deep Web são necessários navegadores específicos, um exemplo é o TOR (The Onion Router), pois com ele é possível identificar a criptografia das páginas com terminação onion, por exemplo. Onion significa cebola,

que faz alusão às camadas presentes nessa “Under Web”, que se acredita ser constituída por diferentes camadas de criptografia.

Muitas pessoas usam tal rede por pura curiosidade, mas conforme citado anteriormente, para manter o anonimato e privacidade, muitos profissionais a utilizam como ferramenta de trabalho, como por exemplo, os jornalistas ao divulgarem notícias polêmicas ou chocantes, policiais no mundo inteiro para investigar crimes, pesquisadores para discutir temas delicados como células-tronco embrionárias, ou seja, pessoas que sentem a necessidade de proteção nominal.

A Web dos anos 90 é muito semelhante a atual Deep Web em termos de popularidade. É preciso conhecer bem as formas de manter a privacidade e o anonimato na Internet, pois a vigia funciona como um sistema de controle e opressão, portanto, a divulgação de formas alternativas de se navegar é necessária. A Deep Web permite uma navegação anônima, o que é útil em lugares cuja liberdade de expressão não existe e a ditadura da informação prevalece. Segundo o coordenador do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas, Carlos Affonso Pereira de Souza, a Primavera Árabe foi organizada principalmente através da Deep Web. (LOPES, 2013). A vantagem de se permanecer oculto no mundo da Internet é que as informações pessoais permanecerão “secretas”, e a vida dos indivíduos não será exposta sem o devido consentimento.

O uso dessa rede paralela vem crescendo cada vez mais com o passar dos anos, mas ainda sim, existem muitos usuários que não sabem que ela existe ou se quer sabem, ou até mesmo desconhecem as formas de acesso. Observando a história da Internet percebe-se que a Deep Web tem um destino muito semelhante, onde as pessoas logo começarão a fazer uso de tal rede, da mesma maneira que a World Wide Web é utilizada atualmente.

É possível fazer uma pesquisa rápida na Web sobre tal assunto, e os primeiros resultados da busca irão mostrar apenas o lado obscuro dessa rede, e também será aconselhado que as pessoas não a utilizem. Devido a esse grande receio, a sociedade prefere utilizar a Web que está acostumada. Eliminar esse preconceito é necessário, pois quanto mais gente utilizando, mais haverá pesquisas e desenvolvimento na área, assim muito mais conhecimento será criado e compatilhado, e assim como a Web em seu início, a Deep Web começará a fazer parte de cotidiano das pessoas, e assim tudo o que deixa as pessoas com medo poderá ser mais controlado.

Todo este contexto histórico e operacional motivou a realização desta pesquisa, a qual foi realizada com a finalidade de informar e orientar o acesso a rede conhecida como Deep Web, para que a mesma possa ser acessada corretamente e com segurança, bem como apresentar o lado bom da rede, para que os preconceitos possam ser quebrados.

2 OBJETIVOS

Apresenta-se abaixo o objetivo geral e os objetivos específicos da pesquisa.

2.1 OBJETIVO GERAL

Demonstrar a melhor maneira de trabalhar com a Deep Web e, ao mesmo tempo, apontar suas principais vulnerabilidades, apresentando formas de acesso com e sem segurança, utilizando os Sistemas Operacionais Windows 7 e Linux Tails.

2.2 OBJETIVOS ESPECÍFICOS

a) Apresentar a Deep Web e seu funcionamento;
b) demonstrar as diferenças entre a Deep Web e a World Wide Web;
c) pesquisar softwares e técnicas de invasão para cada navegador que será utilizado no acesso à deep web;
d) criar um vírus;
e) simular uma situação de utilização com e sem proteção para detectar vulnerabilidades utilizando os sistemas operacionais Windows 7 e Linux Tails, e demonstrar a funcionalidade de ataque contra os mesmos;
f) analisar através de referencial teórico e estudo de caso, a principal vulnerabilidade encontrada;
g) estabelecer um comparativo entre os sistemas operacionais aqui abordados, mostrando as vantagens de desvantagens de se trabalhar com a Deep Web em cada um deles.

3 FUNDAMENTAÇÃO TEÓRICA

Apresenta-se fundamentação teórica utilizada no desenvolvimento da pesquisa.

3.1 INTERNET

A Internet é formada por redes que se comunicam entre si. Uma rede é um conjunto de dispositivos que trocam informações. Até os anos 60 os computadores de fabricantes diferentes eram incapazes de estabelecer uma comunicação, então a ARPA (Advanced Research Projects Agency), que pertencia ao Departamento de Defesa (DOD) do EUA, procurava uma forma dos pesquisadores trocarem informações para reduzir custos e eliminar esforços duplicados. Em 1969 surgiu uma rede formada por quatro universidades norte-americanas, o que deu início à atual rede mundial de computadores. Hoje em dia, para se acessar a Internet os usuários utilizam os provedores de serviços, os quais começaram a surgir em 1995. (FEGAN; FOROUZAN, 2009).

Ainda segundo o autor supracitado, a World Wide Web, ou apenas Web, foi criada pelo CERN (European Laboratory for Paticle Physics), para que fosse possível utilizar os recursos disponíveis em pesquisas científicas.

Para que os computadores pudessem se conectar e estabelecer uma comunicação foi necessário criar uma linguagem para que isso fosse possível. Esta linguagem foi chamada de protocolo. O protocolo é um conjunto de regras e procedimentos que visam a emissão e recepção de dados em uma rede. (COMER, 2006).

De acordo com Comer (2006), na Internet é utilizado protocolo TCP/IP (Transmission Control Protocol/Internet Protocol), que se caracteriza por ser uma sequência de protocolos, um conjunto das regras de comunicação na Internet, e baseia-se no endereçamento IP, isto é, um computador fornecer um endereço IP a cada máquina da rede a fim de poder transmitir pacotes de dados. Cada computador de uma rede possui um endereço IP que é único na rede, é com ele que se identifica uma máquina.

A Web é um serviço no qual o cliente (usuário) através de um browser (navegador) acessa um arquivo disponível num servidor. (WETHERALL; TANENBAUM, 2011).

Um site é acessado quando sua URL (Uniform Resource Locator) é solicitada. Uma URL é um padrão para especificar a localização de uma página na Internet. Wetherall e Tanenbaum (2011) ainda ressaltam que uma URL é uma cadeia de caracteres composta por quatro partes, são elas:

a) O nome do protocolo: Definido pela linguagem utilizada na rede. O mais utilizado é o HTTP (Hyper Text Transfer Protocol). O objetivo do protocolo HTTP é permitir uma transferência de ficheiros que são localizados através de uma cadeia de caracteres chamada URL entre um navegador e um servidor Web;
b) Host: É o nome do servidor. Trata-se do um apelido do computador que armazena a página solicitada;
c) O número de porta: É um número associado a um serviço que permite ao servidor saber o que está sendo pedido;
d) O caminho de acesso ao arquivo: O lugar (diretório) e o nome do arquivo pedido. Existe a dificuldade em se localizar um recurso na Internet através do endereço de IP, então é necessário associar esses endereços numéricos a nomes em linguagem comum através de um sistema chamado DNS (Domain Name System). Quando uma pesquisa é feita, o cliente envia uma mensagem e os buscadores rastreiam o endereço IP relacionado ao DNS procurado, e por sua vez, os servidores enviam uma resposta e exibem os resultados encontrados.

3.2 CRIPTOGRAFIA

Criptografia é o estudo de técnicas matemáticas que proporciona a segurança da informação, evitando que arquivos sejam acessados por pessoas não autorizadas. (MENEZES; OORSCHOT; VANSTONE, 1996).

Uma mensagem texto original é chamada de texto claro, e quando ela é codificada passa a ser chamada de texto cifrado, e esse processo de converter o texto claro em cifrado se chama criptografia. (STALLINGS, 2007).

Quando um documento é criptografado, é criado um código que funciona como uma chave para ler o documento. Existem dois tipos de criptografia: simétrica e assimétrica. A simétrica gera uma única chave, enquanto a assimétrica gera duas chaves, uma para criptografar e outra para descriptografar. (STALLINGS, 2007).

3.3 ROTEAMENTO

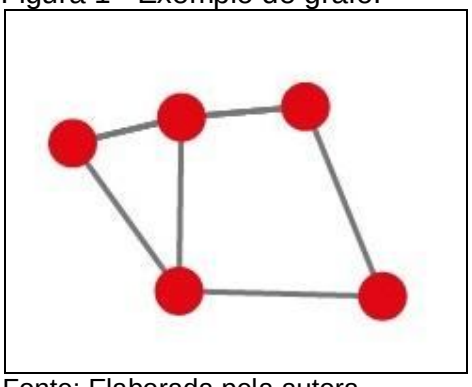
O encaminhamento de pacotes entre as redes que estão interconectadas é feito através de um equipamento chamado roteador, que tem por finalidade determinar o melhor caminho a ser seguido para que seja feito o encaminhando dos dados.

Segundo Comer (2006), o sistema de roteamento da Internet é baseado em proxy. Um servidor proxy é um computador que funciona como mediador entre um navegador da Web e a Internet. É armazenada no servidor uma cópia de resposta para um possível pedido, como é reduzida a carga do servidor original, o tráfego diminui e a latência é melhorada. Cada máquina ligada em uma rede possui switch, que é um dispositivo que seleciona qual será o caminho que um pacote fará para chegar ao seu destino.

O switch localiza onde a máquina procurada se encontra na rede para que a permuta de informações possa acontecer. Essa distribuição de pacotes é chamada de roteamento. Na Internet um switch está ligado a várias redes, portanto o emissor e o destinatário devem pertencer à mesma rede em uma entrega de pacotes direta, e em uma entrega indireta existe pelo menos um switch entre ambos. Quando o switch encontra o endereço do destinatário a mensagem é transmitida. (COMER, 2006).

A conexão entre as máquinas pode ser demonstrada através de um grafo. Um grafo é formado por vários pontos conectados por linhas, onde os pontos são os vértices e as linhas são as arestas. O grafo ilustrado na Figura 1 possui cinco vértices e seis arestas.

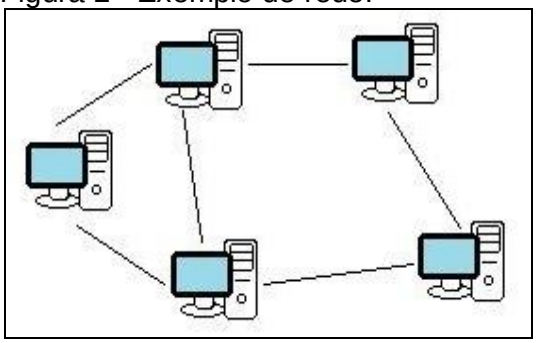
Figura 1 - Exemplo de grafo.



Fonte: Elaborada pela autora.

Quando da comunicação entre computadores, os vértices são as máquinas e as arestas representam a conexão entre as mesmas, conforme ilustra a Figura 2:

Figura 2 - Exemplo de rede.



Fonte: Elaborada pela autora.

Conforme pode ser observado, as Figuras 1 e 2 são equivalentes, pois possuem o mesmo número de pontos e ligações.

3.3.1 Roteamento Cebola

É um sistema de encaminhamento de pacotes em uma rede, que tem por objetivo fornecer uma navegação privada e anônima no sentido de que tanto a própria rede, como qualquer intruso não possa identificar o conteúdo, e nem mesmo o tráfego das mensagens entre o remetente e o destinatário.

Tal sistema de roteamento foi proposto pela primeira vez na década de 80 por David Chaum e foi chamado de Chaum Mixes ou Mix Networks.

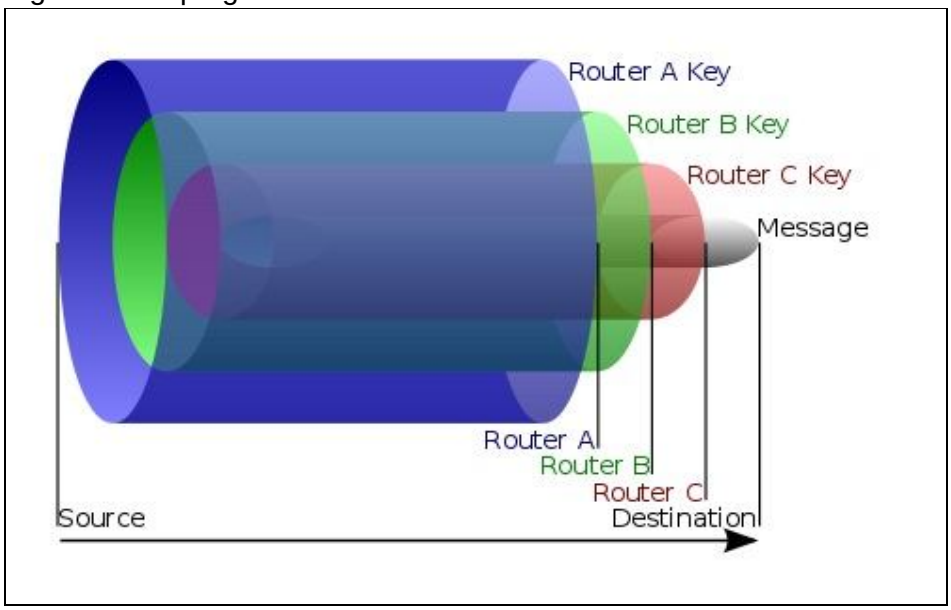
Nesse tráfego de informações não se faz uma conexão diretamente à máquina destino. Cria-se a comunicação utilizando uma cadeia de servidores proxy, ou seja, uma máquina aleatória é selecionada para ser utilizada como proxy. Deste modo é construída uma conexão anônima através de vários roteadores cebola até o destino. Cada Onion Router identifica o nó mais próximo ao longo do caminho. (GOLDSCHLAG; REEDY; SYVERSON, 1999, tradução nossa).

Segundo os autores supra citados, antes das informações serem transmitidas, as mesmas são divididas em partes, onde cada uma recebe uma camada de criptografia no pacote a ser enviado, assim, cada Onion recebe uma chave para decifrar a mensagem até ser transformada em um texto simples. Para que esse texto chegue ao destino, todas essas camadas devem ser totalmente decifradas.

Assim que o destino final é alcançado, uma resposta é transmitida ao solicitante. Posteriormente a conexão aparece diferente em cada Onion Router, para que os dados não possam ser rastreados. Quando a conexão é quebrada ou finalizada, todas as informações são eliminadas. É essa adição de camadas de criptografia que faz alusão à criação de uma cebola, também chamada de hop, e quando são descriptografadas diz-se que elas são descascadas. (DINGLEDINE; MATHEWSON; SYVERSON, 2004, tradução nossa).

A Figura 3 demonstra o sistema de criptografia cebola, onde a camada azul da figura é a origem do pacote, e a mensagem passa por vários nós, representados pelas camadas sequentes, mantendo a mensagem em seu interior, que só será exibida se as chaves forem decifradas. Conforme pode ser observado na Figura 3, a camada azul representa a origem da mensagem que posteriormente passa por três nós onde cada roteador adiciona uma camada de criptografia, gerando uma chave que será fornecida para próxima camada, assim, quando a mensagem chega ao seu destino final, o pacote será decifrado em conjunto.

Figura 3 - Criptografia Cebola.



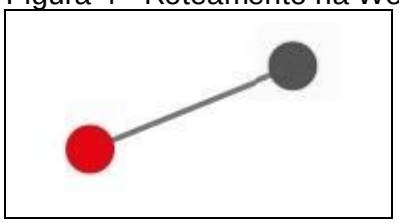
Fonte: Wikipedia (2014).

Existem poucas diferenças entre o Chaum Mixes e a primeira geração do Onion Router. As principais são: no Chaum os pacotes são enviados todos para um servidor que os embaralha e redistribui aleatoriamente, e quando a chave é

traduzida o endereço destino é revelado. (CHAUM, 1981, tradução nossa). Com o Tor o endereço permanece oculto, e quando se chega ao destino final uma nova cebola é gerada para que então a resposta se transmitida.

Se for feita uma comparação entre o roteamento tradicional da internet e o roteamento cebola, nota-se que no roteamento da Web a conexão acontecerá diretamente ao servidor que o serviço solicitado está armazenado, conforme indica a Figura 4, onde o ponto vermelho é a origem e o cinza escuro é o destino.

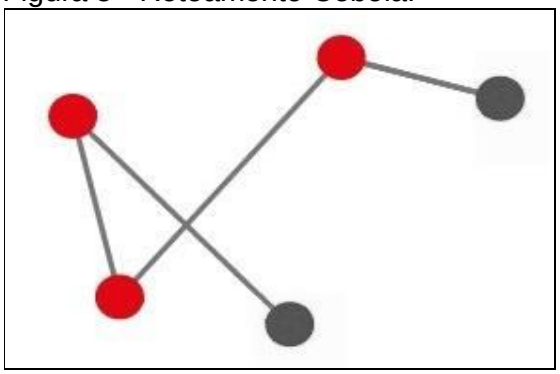
Figura 4 - Roteamento na Web.



Fonte: Elaborada pela autora.

No roteamento cebola os pacotes irão passar por vários nós antes de chegar ao seu destino, conforme ilustra a Figura 5, onde os nós cinza escuros podem ser origem ou destino final, e os pontos vermelhos representam o nós por onde os pacotes passam antes de alcançar o destino final.

Figura 5 - Roteamento Cebola.



Fonte: Elaborada pela autora.

3.4 ARQUITETURA P2P

A abreviatura P2P (peer-to-peer) é utilizada para caracterizar redes onde as máquinas que a compõem são servidores e clientes ao mesmo tempo, o que permite o compartilhamento de serviços e dados sem a necessidade de um servidor central.

Cada computador é um nó, ou seja, um ponto de interconexão. Todos os computadores da rede devem usar programas compatíveis para que a conexão entre os mesmos aconteça adequadamente, e é dividido entre cada um o poder de processamento, largura de banda e armazenamento de arquivos. Uma rede peer-to-peer pode ser usada para compartilhar qualquer arquivo digital. (FEGAN; FOROUZAN, 2009).

Na internet existem softwares para compartilhamento de informações que utilizam tal arquitetura. Quando um usuário faz o download de um arquivo, ele não está baixando tal conteúdo de um único servidor central, e sim uma fração de vários computadores que possuem aquele arquivo armazenado. Quando o download estiver completo o cliente também será um servidor. Quanto mais máquinas possuírem tal arquivo mais rápido será o download.

3.5 DEEP WEB

A Deep Web está ligada à internet. Pelo fato das páginas não serem localizadas por provedores de busca comuns, seu conteúdo fica oculto na rede. O termo Deep Web foi utilizado pela primeira vez pelo cientista Michael K. Bergman, e segundo ele é uma evolução da Web sendo inicialmente formada por sites obsoletos e inutilizados. (LAMARÃO; MELONIO; LAMARÃO, 2013). Os usuários começaram utilizá-la para fugir da vigia e monitoração, compartilhando informações e arquivos que não poderiam estar na Internet comum. O termo Deep Web, significa web profunda, fazendo referência à pesca, onde é possível encontrar mais peixes no fundo do oceano do que na superfície. (BERGMAN, 2001, tradução nossa).

Por exemplo, se for elaborada uma pesquisa com as palavras “energia nuclear” serão exibidas páginas que possuem o vocábulo solicitado, essas páginas estarão presentes na Surface Web, um termo técnico que indica um conjunto de páginas facilmente localizadas por mecanismos de busca. (POMPÉO; SEEFELDT, 2013).

Uma das principais diferenças entre a Surface Web e a Deep Web é o fato das páginas desta segunda não serem indexadas aos motores de busca comuns, ou seja, buscadores como o Google ou Yahoo não localizam os sites da Deep Web, mesmo que a página possua o conteúdo procurado. (BERGMAN, 2001, tradução nossa). Isso acontece propositalmente, ou porque o programador não quer que a

página seja localizada por tais ferramentas, ou ainda porque a página não é estática, ou seja, seu conteúdo é criado dinamicamente no momento em que a mesma é acessada.

Alguns dos motivos que levam as páginas a não serem indexadas são:

a) O fato delas possuírem conteúdo privado sendo necessário uso de login e senha para evitar que informações sejam passadas para desconhecidos;
b) ou o proprietário da página optar pela privacidade, ou até mesmo, o conteúdo da mesma ser categorizado como conteúdo impróprio.

O conteúdo impróprio pode ser a violação de direitos autorais, fotos e vídeos exibindo cenas violentas, divulgação de informações confidenciais, ou seja, qualquer informação que viole as regras dos buscadores pode ser considerada como conteúdo impróprio.

Para que o acesso a tal recurso seja bem sucedido, é necessário o uso de softwares específicos que acessem as páginas através de um sistema de roteamento diferenciado. Pode ser utilizado o roteamento cebola, uma rede ponto a ponto, ou uma combinação de roteamento com rede ponto a ponto, chamada i2P.

A presença de softwares de navegação privada em diversas máquinas faz alusão a uma rede, pois a comunicação dá-se entre os computadores interligados através dos nós que possuem um navegador específico, portanto, a Deep Web está presente na World Wide Web, a diferença é que são utilizados túneis de comunicação diferentes para transferência de dados.

3.5.1 Softwares de navegação

Para que o acesso anônimo à internet seja bem sucedido é necessário o uso de navegadores e softwares específicos com as características de roteamento e arquitetura já apresentadas. A seguir apresentamos os browsers e, o complementos dos mesmos, que foram utilizados para estudo e análise neste trabalho.

3.5.1.1 Tor (The Onion Router)

É um navegador baseado no roteamento cebola, que visa o anonimato do usuário. Segundo o site oficial do projeto, seu desenvolvimento iniciou em 1995. Era financiado pela ONR (Office of Naval Research), e sua apresentação formal inicial foi em 31 de maio de 1996. O código foi aprovado para distribuição pública em julho. Em 1997 passou a ser financiado também pela DARPA (Defense Advanced Research Projects Agency). Em 1998 a primeira rede foi criada com 13 nós. A patente do Tor foi emitida em 2000, e em dois anos de funcionamento houve 20 milhões de processamentos em 60 países diferentes através do Onion Router. (SYVERSON, [2005?], tradução nossa).

Segundo Syverson ([2005?]) essa foi a primeira geração, que foi abandonada em 2002 por ser muito antiquada, e então começou a ser desenvolvida a Segunda Geração. Com o desenvolvimento da internet como um todo, o código pôde ser desenvolvido com mais simplicidade, pois muitas coisas puderam ser aproveitadas, como por exemplo, o desenvolvimento dos proxies e o aumento de números de endereço IP.

Syverson ([2005?]) explica ainda que em 2003, o projeto passou a ser financiado pela NRL (Naval Research Laboratory), então o código foi implantando e liberado para o MIT (Massachusetts Institute of Technology), logo uma rede foi criada com mais ou menos 12 nós voluntários na Alemanha e Estados Unidos. No ano de 2004, a ONR e a DARPA interromperam a concessão de fomento ao projeto, e logo em seguida, a FEP assumiu então o financiamento, implantação e desenvolvimento da rede.

De acordo com Haddow (2012), o Tor era usado principalmente pela marinha dos EUA, e foi distribuído para que mais pessoas pudessem utilizá-lo como uma forma de disfarce, pois se fosse utilizado apenas para fins militares, sempre que uma mensagem que tivesse a criptografia onion fosse interceptada, o interceptor saberia que havia encontrado uma informação da Marinha dos EUA.

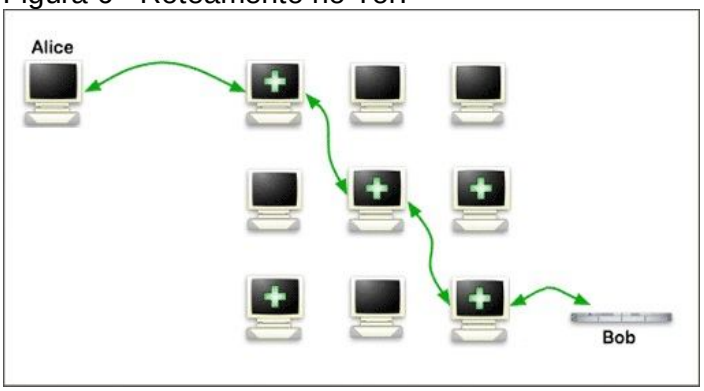
O Tor foi baseado no Chaum Mixes e teve algumas modificações. No Chaum Mixes, o Roteamento Cebola original, era necessário um nó hostil para identificar e armazenar o tráfego para comprometer os próximos nós e fazer a decodificação do tráfego. (GOLDSCHLAG; REEDY; SYVERSON, 1996, tradução nossa). No Tor, em vez da cebola ser gerada e descriptografada, suas chaves vão sendo geradas ao

longo do tráfego. A rede Tor é formada por mais de 3600 servidores que atuam voluntariamente. A conexão passa por três nós antes de chegar ao seu destino final. (LEE, 2013).

De acordo com as informações retiradas do site oficial do projeto Tor, nenhum nó conhece o caminho que o pacote percorreu, e as ligações em circuitos criados em um intervalo de até 10 minutos, evitando relações de ações prévias com as novas. (TOR, [2004?]).

A Figura 6 demonstra um caminho percorrido pelos pacotes no Tor, onde Alice quer uma conexão com Bob, o que não ocorre diretamente, e sim passa por vários nós antes de se chegar ao destino final.

Figura 6 - Roteamento no Tor.



Fonte: Site Tor Project (2014).
Nota: Adaptado pela autora.

3.5.1.2 Freenet

Proposto por Ian Clarke em 1999 e apresentado em 2002, o Freenet é um software que forma uma rede onde vários usuários contribuem com o compartilhamento de mensagens, arquivos e diversas informações. É baseado na arquitetura de rede P2P que permite a publicação, replicação e recuperação de dados mantendo o anonimato do autor e do receptor dos dados. Ele funciona como uma rede de nós idênticos que armazenam dados coletivamente e coopera para rotear pedidos para as máquinas destino. (CLARKE et al., 2000, tradução nossa).

Seu funcionamento é feito a partir da contribuição entre os usuários, com diversos nós idênticos. Atuando como complemento de outro navegador, a sua arquitetura descentralizada aumenta a robustez da rede e diminui os pontos de falha.

Todo usuário fornece um espaço para armazenamento, transformando a máquina em um servidor. Quando um usuário adiciona um novo arquivo, uma mensagem é enviada

na rede informando a localização através de um identificador, uma chave chamada GUID. Para recuperar o arquivo, um usuário envia uma mensagem de solicitação que contém a chave GUID. Quando o pedido chega a um dos nós onde o arquivo está armazenado, esse nó transmite os dados ao solicitante. (CLARKE et al., 2002, tradução nossa).

3.5.1.3 i2P

O sistema I2P (Invisible Internet Project) não é um navegador independente, ou seja, ele funciona junto com outro navegador. O I2P possui as características do roteamento cebola no que diz respeito ao envio de pacotes e da arquitetura P2P quanto à troca de arquivos entre os usuários. De acordo com Ehlert (2011, tradução nossa), O projeto i2P foi proposto pela primeira vez em 2003, e foi baseado no Invisible Internet Project (IIP), um sistema de comunicação anônimo em tempo real.

O i2P utiliza túneis para comunicação entre os usuários. Cada túnel é definido por 3 nós: o gateway, que é uma máquina intermediária, o participante e o final. Para que a troca de dados aconteça, é necessário que a mensagem seja enviada para o nó gateway do túnel onde o nó final é o solicitado. (EHLERT, 2011, tradução nossa). Os túneis tem uma duração de dez minutos, logo, para que o usuário possa manter a conexão à rede os túneis devem ser constantemente recriados. (EGGER et al., 2013, tradução nossa).

Para que cada usuário possa enviar mensagens para os outros, este deve ter algumas informações sobre os túneis. Para isso, o sistema I2P possui um mecanismo chamado NetDB (Network Database) - uma base de dados distribuída que oferece metadados para que a comunicação entre usuários seja possível. São esses o metadados:

a) RouterInfo: informações sobre como contatar um nó e suas estatísticas;
b) LeaseSet: informações sobre como contatar um destino.

Estes dados são fornecidos pelos próprios usuários. Para a criação de um túnel, o NetDB envia mensagens encriptadas para os nós selecionados para criação do mesmo. Cada mensagem possui uma chave para cada nó onde apenas esse nó terá acesso ao conteúdo das mensagens. Cada contribuinte escolhe o comprimento dos túneis a serem utilizados, posteriormente, acontece a troca entre o anonimato, latência e taxa de transferência de dados. (SCHIMMER, 2009, tradução nossa).

3.6 MALWARES

Significa “malicious softwares”, ou seja, são softwares maliciosos que se instalados no computador podem causar danos à máquina, alteração no conteúdo e roubo de informações. (GRÉGIO, 2012).

Esses malwares são utilizados para manter a máquina vulnerável, para que um ataque seja possível. Instalar programas em computadores é uma das técnicas de invasão utilizada pelos atacantes. Os malwares podem ser divididos em várias categorias, a seguir podem ser verificadas algumas delas.

3.6.1 Vírus

Os vírus se propagam fazendo cópias de si mesmo e se tornando parte de outros programas ou arquivos executáveis. Eles permanecem inativos até que o usuário instale o programa infectado. Quando a máquina se transforma em um hospedeiro, o vírus se espalha de um computador para outro através de e-mails ou outros tipos de transferência de arquivos. (ZELTSER; SKOUDIS, 2004, tradução nossa).

3.6.2 Worms

Do inglês verme, os worms possuem um comportamento semelhante aos vírus, mas segundo Zeltser e Skoudis (2004, tradução nossa), a diferença entre ambos é que o worm é um programa independente, ou seja, não é anexo a outro software e, também, não necessita de interação com o usuário.

3.6.3 Trojan

Fazendo referência a estratégia grega, o Cavalo de Troia é o componente de um programa. A diferença entre os malwares já citados, é que o Cavalo de Troia se faz passar por um programa útil, ocultando sua verdadeira finalidade. (ZELTSER; SKOUDIS, 2004, tradução nossa).

3.6.4 Rootkits

São geralmente indetectáveis e combinados com outros tipos de malwares. São utilizados para permitir o acesso remoto para o atacante e tornar o código difícil para a vítima de detectar. (SIKORSKI; HONIG, 2012, tradução nossa).

3.6.5 Spywares

Spy em inglês significa espião, a característica principal destes programas que, quando instalados, monitoram o comportamento da máquina infectada. Em posse das informações adquiridas, o usuário se torna um alvo mais fácil para o atacante. (GRÉGIO, 2012).

3.6.6 Backdoor

O código se instala em um computador para permitir o acesso atacante. Ele pode ser um programa autônomo ou estar incorporado em outro programa. (GRÉGIO, 2012).

3.6.7 BotNet

Quando vários computadores em uma rede estão infectados por um programa com comportamento semelhante ao backdoor, a rede é remotamente controlada pelo mesmo invasor. Tal comportamento é chamado de BotNet. (SIKORSKI; HONIG, 2012, tradução nossa).

3.7 SEGURANÇA DA INFORMAÇÃO

Segurança da Informação diz respeito à proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade. (SILVA; CARVALHO; TORRES, 2003).

O princípio da Disponibilidade é garantido quando a informação está acessível sempre que necessário. O princípio da Integridade é garantido quando a

informação acessada está completa, sem alterações e portanto confiável. O princípio da Confidencialidade é garantido quando apenas as pessoas explicitamente autorizadas podem ter acesso a Informação. O princípio da Autenticidade é garantido quando se confia que a pessoa que está realizando uma ação é realmente a pessoa que diz ser. (SILVA; CARVALHO; TORRES, 2003).

A segurança da informação é importante para proteger os dados e informações pessoa. Quando uma pessoa utiliza a internet ela pode ficar vulnerável e exposta a certas e ameaças, como roubo de senhas, por exemplo.

Um das formas de assegurar a integridade dos dados pessoais na internet é através de programas específicos para isso.

3.8 SOFTWARES DE SEGURANÇA

Devido a existência de grandes chances de falhas e vulnerabilidades em programas utilizados para o acesso à internet, de uma forma geral, é necessário tomar alguns cuidados quando é feito o acesso, como não clicar em links desconhecidos, e não fazer download de arquivos com o formato .exe (executável) por exemplo. Mas mesmo tomando os devidos cuidados existe ainda um alto risco de uma máquina ser infectada por malwares e sofrer ataques de hackers.

Além dos cuidados a serem tomados, é necessário o uso de softwares específicos que evitem que a máquina seja infectada por vírus e que sofra alguma invasão. A seguir serão apresentados alguns softwares que auxiliam a potencialização da segurança.

3.8.1 Antivírus

São programas que visam a prevenção, detecção e exclusão de malwares. Também possuem a função de barrar programas suspeitos, impedir downloads e acesso a sites que apresentam possíveis ameaças. (SILVA; CARVALHO; TORRES, 2003).

3.8.2 Firewall

Traduzido para o idioma português, firewall significa parede de fogo. Sua

função é inspecionar todos os pacotes que transitam a rede. Se o pacote se encaixa nos critérios a que está submetido, será enviado normalmente. (ZWICKY; COOPER; CHAPMAN, 2001).

3.10 SISTEMAS OPERACIONAIS

São programas que gerenciam os recursos do computador e fornecem base para a execução dos softwares instalados na máquina. (SILBERSCHATZ; GALVIN; GAGNE, 2010). Existem várias versões de sistema operacional, as enumeradas neste trabalho são listados a seguir.

3.10.1 Windows 7

Foi em 1981 que o primeiro PC com o sistema operacional MS-DOS começou a ser comercializado. Como era difícil para as pessoas entenderem, foi criado um SO (sistema operacional) que dispensava o uso de comandos em linhas de código. Em 1985 o Windows 1.0, que recebeu esse nome por causa das janelas fundamentais nesse novo sistema, começou a ser comercializado. (UMA HISTÓRIA..., 2013). O Windows 7, é por enquanto a versão mais utilizada no mundo segundo a Netmarketshare (REALTIME, 2014, tradução nossa).

3.10.2 Linux Tails

A primeira versão do Linux foi lançada em setembro de 1991 por Linus Trovalds. (TANENBAUM, 2010). Desenvolvido como um hobby, o que motivou a execução do projeto foi a frustração de Linus diante dos sistemas utilizados na universidade.

Com código aberto, o Linux possui inúmeras versões, sendo programado por desenvolvedores no mundo inteiro. Uma dessas versões é o Tails - The Amnesic Incognito Live System.

Baseado em Debian, sistema operacional que utiliza o Linux kernel, o foco do Tails é preservar a privacidade e o anonimato. É portátil, ou seja, não necessita instalação, e pode ser usado independente do sistema operacional presente no computador. (SOBRE, [2014?]).

Em conformidade com o site Tails ([2014?]), o Tails é configurado para acessar a internet utilizando o Tor, portanto qualquer outro aplicativo que tentar uma conexão direta será bloqueado, bem como, conexões ponto a ponto já que o IP de origem não é revelado.

O Tor oculta a localização do usuário, mas não existe garantias de que a comunicação será preservada, no entanto, o Tails é inteiramente configurado para criptografar todos os dados que serão emitidos pela máquina. (SOBRE, [2014?]).

Ainda, segundo o site supracitado, o Tails utiliza apenas a memória RAM[2] do computador que, quando desligado, não deixa rastros, daí o nome amnésico.

3.11 MÁQUINA VIRTUAL

Tanenbaum (2010) diz que uma máquina virtual é uma cópia exata do hardware. A impressão que se passa na execução de uma máquina virtual é que um ambiente é executado dentro de outro ambiente separado, ou seja, uma máquina dentro de outra.

As máquinas foram comercializadas pela primeira vez pela IBM através do sistema operacional VM em 1972, o VM370. Era executada em um mainframe dividido em várias máquinas virtuais, cada um com um sistema operacional. (SILBERSCHATZ; GALVIN; GAGNE, 2010).

Ainda segundo os autores acima, existem vários benefícios na criação de uma máquina virtual, dentre eles é o compartilhamento de hardware e a execução de vários ambientes diferentes simultaneamente, e ainda, o sistema hospedeiro fica protegido, pois as máquinas virtuais ficam isoladas umas das outras.

Já que uma máquina não interfere no funcionamento de outra, um vírus ou uma tentativa de invasão dentro de um sistema operacional convidado não irá afetar a máquina em que o sistema operacional está sendo executado.

Para a execução de uma máquina virtual faz-se o uso de softwares específicos que emulam um sistema operacional na máquina em que está instalado.

[2] A memória RAM é o componente do computador que permite a leitura e gravação de dados na máquina para a execução de tarefas. É volátil, ou seja, quando a máquina é desligada, as informações armazenadas na memória RAM são apagadas.

3.12 O MOVIMENTO CYPHERPUNK

Criptografia significa escrita escondida, o que permite a comunicação através de códigos, e a tradução de cypherpunk para o português pode ser criptopunk. O movimento Cypherpunk foi criado em 1990 e defende o uso da criptografia e métodos semelhantes para que mudanças políticas e sociais possam acontecer, e sua filosofia fundamental é “privacidade para os fracos, transparência para os poderosos”. (ASSANGE et al., 2013).

Julian Assange, um dos precursores do movimento, é o criador da WikiLeaks, um site que expõe documentos secretos de governos no mundo inteiro, e publica notícias que são censuradas na maioria dos países. Ele condena a espionagem e a restrição de informações à população, e defende a filosofia hacker: a informação deve ser livre. (VIANA, 2013 apud ASSANGE et al., 2013, p. 11).

Segundo Assange et al. (2013, p. 28): “A missão do WikiLeaks é receber informações de denunciantes, divulgá-las ao público e se defender dos inevitáveis ataques legais e políticos.”

A internet pode facilitar a comunicação, mas também facilita a vigilância, o que tem sido facilitado ainda mais com as pessoas divulgando suas opiniões e dados pessoais por livre e espontânea vontade em redes sociais, por exemplo. Os cypherpunks sempre conheceram o poder da informação, os que detêm conhecimento são detentores do poder.

Como a informação é uma ferramenta poderosa para manipulação, existem muitos órgãos que armazenam e buscam informações pessoais de pessoas ao redor do mundo através de espionagem. É para proteger a privacidade das pessoas que o movimento cypherpunk se mobiliza e, uma das formas das pessoas se protegerem é utilizando meios de comunicação que oculte a própria identidade e localização.

Como a característica fundamental do Tor é o anonimato, os adeptos ao movimento cypherpunk apoiam e incentivam o uso do mesmo, pois é o navegador que permite a privacidade que mais se adequa à filosofia hacker.

4 METODOLOGIA

O propósito das pesquisas exploratórias é proporcionar ao investigador maior familiaridade com o problema, objetivando torná-lo mais explícito ou construir hipótese. Uma pesquisa de cunho exploratório tende a ser bastante flexível, pois leva em consideração os mais variados aspectos relativos ao problema estudado. De modo geral, pesquisas realizadas com propósitos acadêmicos, pelo menos inicialmente, assumem esse caráter exploratório, pois neste momento é pouco provável que o pesquisador tenha uma definição clara do que irá investigar. (GIL, 2010).

A produção deste trabalho exibe uma série de etapas que devem ser seguidas até a obtenção dos resultados, os quais se pautam na análise de técnicas e de software de navegação voltado para o acesso à internet anonimamente.

De acordo com o funcionamento da Deep Web apresentado no referencial teórico, foram analisadas as vulnerabilidades dos riscos de ataques que os usuários estão expostos ao utilizar tal rede de comunicação. Para isso, foi necessário entender como funciona um dos processos de invasão através do uso de navegadores que mantém o anonimato na rede. Logo, foram realizadas tentativas de invasão para descobrir em quais situações uma máquina fica vulnerável. Essas tentativas foram elaboradas com fins estritamente acadêmicos.

As tentativas foram focadas no navegador Tor, já que o Freenet e o I2P são baseados em trocas de chaves e em confiança entre os usuários, sendo mais necessário o bom senso do que conhecimentos específicos para que seja possível uma navegação segura.

A pesquisa foi baseada na Filosofia Estatística da Análise de Variância, que leva em conta a variável e o fator de variação. A variável é a medida do objeto que será avaliado, e o fator de variação é tudo o que provoca alterações nessa variável. A variável deve ser única, enquanto podem haver múltiplos fatores de variação atuando sobre uma variável simultaneamente. A resposta obtida provém das mudanças da variável quando a mesma sofre influência dos fatores de variação. Essa filosofia admite que os efeitos dos fatores de variação possam ser avaliados tanto em conjunto como isoladamente na comparação dos resultados, por isso a aplicação de testes embasados nessa filosofia da estatística podem ser aplicados alternando a variância a cada nova tentativa, evitando a repetição dos critérios.

(CAMPOS, [1997?]). É nesse contexto que foi elaborada a aplicação dos testes, onde a variável é a invasão e os fatores de variação são os ambientes, ou seja, as configurações da máquina a ser invadida, que será explicado a seguir.

4.1 CONFIGURAÇÃO DO AMBIENTE

Para realizar a invasão foi utilizada uma máquina “invasora”, a qual dispõe das seguintes configurações: marca Dell com 4 GB de memória RAM, 500 GB de HD, com o sistema operacional Windows 7, onde foi configurado o software de invasão SpyNet e criado um vírus, que foi criado seguindo os passos descritos no manual que vem junto ao programa. A técnica utilizada para todas as tentativas de invasão foi o cavalo de troia. O tipo de invasão mais comum na internet é por meio de infecções, que acontece com malwares, dentre eles o mais conhecido e mais simples para realização de ataques é o cavalo de troia, sendo assim, o mais utilizado. O software SpyNet foi escolhido para elaboração do trabalho porque é simples e fácil de usar, podendo ser utilizado por qualquer pessoa que não tenha muitos conhecimentos na área de tecnologia da informação.

A máquina invadida possui as mesmas configurações que a citada anteriormente. Essas configurações se referem às máquinas disponíveis para utilização. No que diz respeito ao sistema operacional, o Windows 7 foi utilizado por ser atualmente o mais usado, como já citado no tópico 3.10.1 da fundamentação teórica.

Antes de começar a realização dos testes, foi feito um backup dos arquivos pessoais para evitar a perda de qualquer documento presente na máquina a ser atacada, e também foi feita uma limpeza os navegadores para eliminar senhas salvas, evitando assim que a máquina utilizada para invasão ficasse vulnerável a outros invasores.

Primeiramente foi instalado o antivírus Avast, que foi escolhido por ser grátis e também porque foi considerado um dos melhores antivírus gratuitos de 2014. (TESTE..., 2014). Como o Windows 7 já possui um firewall, não foi necessário a instalação de outro.

Posteriormente foi preciso baixar e instalar o Tor, cujo tutorial de instalação está presente no Apêndice A.

Esses foram os softwares necessários para os testes no Windows 7. Para utilização do Tails foi utilizado um pendrive da marca SanDisk de 8 GB, pois era necessário um pendrive de no mínimo 4 GB. A instalação do Tails aconteceu conforme mostra Apêndice B. O sistema operacional Linux foi escolhido por apresentar algumas características mais seguras, podendo ser utilizado como uma alternativa mais eficiente para manter-se um ambiente mais seguro.

E por último, foi feita a instalação da máquina virtual, conforme Apêndice C. O software Oracle Virtual Box foi escolhido para ser utilizado para emular uma máquina virtual por ser gratuito e de fácil utilização. Não foi necessário instalar o Tor no Tails, pois o mesmo já se encontra presente no sistema operacional. Também não foram utilizados antivírus para Tails devido à existência de poucos, bem como não haver muitas informações sobre eles, e o firewall do mesmo é embutido no próprio sistema.

No site oficial do Tor encontra-se um comunicado explicitando a vulnerabilidade do Windows. (TOR, 2013, tradução nossa). Portanto, o Tails foi escolhido para elaboração dos testes pelo fato de ser um sistema operacional elaborado especificamente para preservar a identidade do usuário, servindo como complemento para o Tor, por exemplo.

As especificações dos ambientes invadidos estão na Figura 7 e serão explicadas com detalhes na próxima seção:

Figura 7 - Descrição dos ambientes

AMBIENTE	WINDOWS 7	TAILS	TOR	ANTIVIRUS	FIREWALL	MAQUINA VIRTUAL
1	X		X	X	X	
2	X		X	X		
3	X		X		X	
4	X		X			
5		X	X			
6	X		X			X

Fonte: Elaborado pela autora (2014).

Para invadir a máquina que é a suposta vítima, foi criada uma conta de email no TorBox, o mesmo possui extensão .onion, portanto só roda no Tor. Nessa conta foi anexado o trojan para que pudesse ser aberto e baixado na máquina a ser a atacada.

4.2 INVASÕES

As invasões foram elaboradas uma vez em cada ambiente descrito no tópico anterior sendo compatível à filosofia da estatística já explicada anteriormente. Os procedimentos realizados se configuram conforme segue abaixo.

4.2.1 Ambiente 1

Nesse primeiro ambiente a máquina com Windows 7 possui antivírus e firewall ativos. O Tor e o email foram abertos, e foi dado início ao download do arquivo.

4.2.2 Ambiente 2

As configurações do antivírus não foram alteradas, mas o firewall foi desativado pelo caminho Botão Iniciar\Painel de Controle\Sistema e Segurança\Firewall do Windows\Personalizar Configurações. Como havia mais de uma rede, o firewall de todas elas foi desativado. O Tor foi fechado e aberto novamente, bem como o TorBox, então o download foi iniciado.

4.2.3 Ambiente 3

O antivírus foi desativado clicando na seta que fica no canto inferior direito da máquina “Mostrar ícones ocultos”, posteriormente clicando com o botão direito do mouse sobre o ícone do Avast, então foi posicionada a seta do mouse sobre a opção “Controle dos módulos do Avast!” e foi selecionada a opção “Desabilitar até que o computador reinicie”. O firewall foi reativado, pelo caminho “Controle\Sistema e Segurança\Firewall do Windows\Personalizar Configurações”. O Tor foi reiniciado e o TorBox foi aberto novamente, para então ser iniciado o download do arquivo novamente.

4.2.4 Ambiente 4

O antivírus foi mantido desativado, e o firewall foi desativado novamente conforme o caminho mostrado nas etapas anteriores. Novamente o Tor e o TorBox foram reiniciados, e o foi iniciado o download do arquivo mais uma vez.

4.2.5 Ambiente 5

Para ser utilizado o Tails, a máquina foi desligada, o pendrive no qual o sistema operacional estava instalado foi colocado na máquina. A máquina foi iniciada e o Linux Tails também. O Tor e o TorBox foram inicializados e o download do arquivo presente no email foi iniciado.

4.2.6 Ambiente 6

Para a máquina virtual foi utilizado o Oracle Virtual Box em sua versão mais recente, e então a máquina virtual Tails foi iniciada. Com o Tor e o TorBox carregados, foi realizado o download do arquivo. Foi utilizada uma máquina virtual como uma alternativa de se manter a máquina protegida.

5 RESULTADOS

As tentativas de invasão foram feitas em cada ambiente, onde cada um obteve uma resposta de sucesso e insucesso de acordo com sua configuração. Segue os resultados.

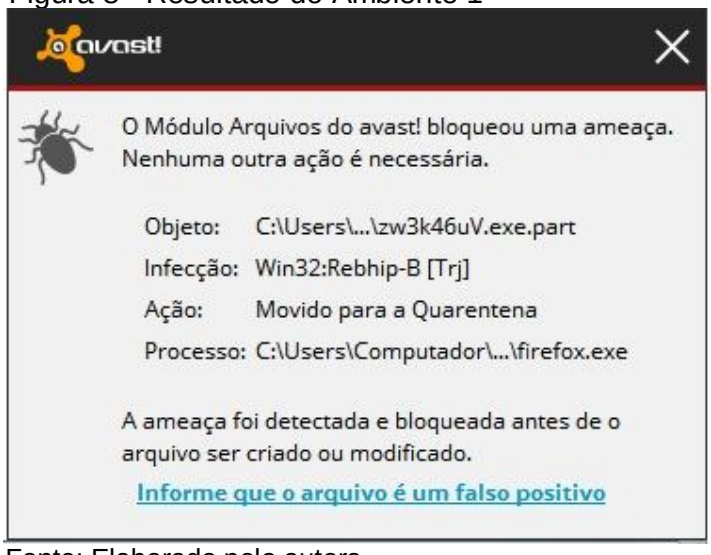
5.1 RESULTADO POR AMBIENTE

Alguns resultados foram semelhantes devido aos ambientes serem semelhantes, mas ao serem observados com atenção nota-se um comportamento diferente em cada um.

5.1.1 Ambiente 1

Nesse primeiro ambiente a máquina com Windows 7 está com antivírus e firewall ativos. O email foi aberto, e foi dado início ao download do arquivo. Conforme mostra a Figura 8, o antivírus bloqueou o download do arquivo no navegador pois foi detectado que o arquivo era malicioso. O processo completo pode ser observado no Anexo A.

Figura 8 - Resultado do Ambiente 1

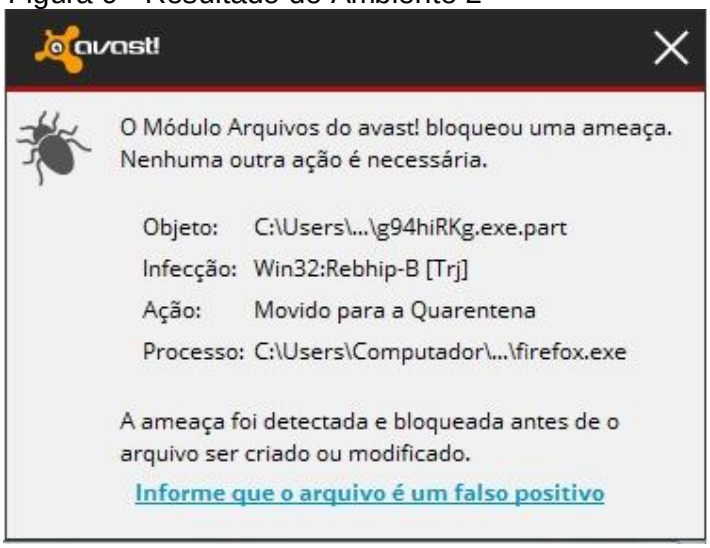


Fonte: Elaborado pela autora.

5.1.2 Ambiente 2

Nesse caso a máquina estava apenas com o antivírus ativo, e assim como no ambiente anterior, o antivírus impediu que o arquivo malicioso fosse baixado, conforme mostra a Figura 9, que está completa no Anexo B.

Figura 9 - Resultado do Ambiente 2

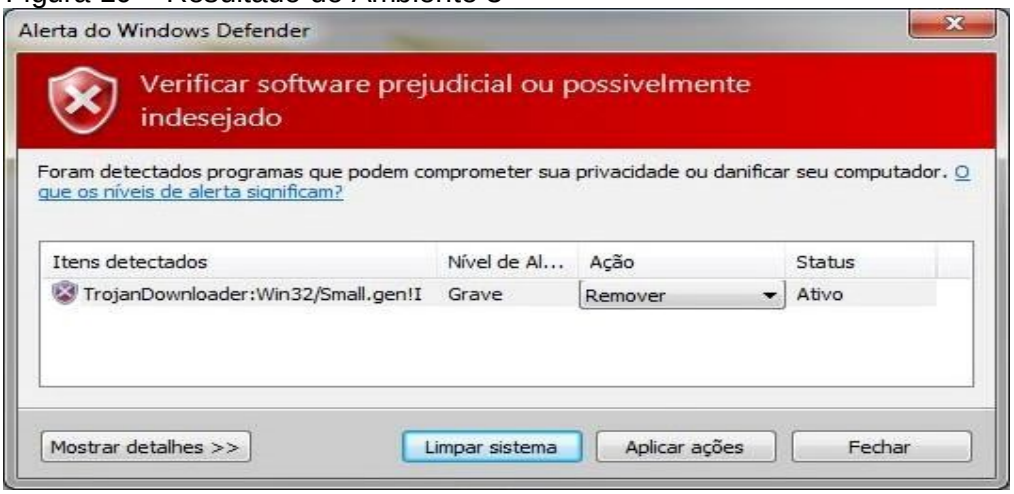


Fonte: Elaborado pela autora.

5.1.3 Ambiente 3

Nesse caso apenas o firewall estava ativo, portanto o arquivo foi baixado e executado, mas o firewall detectou que seria feita uma conexão insegura, portanto bloqueou a finalização de execução do arquivo, impedindo que o ataque fosse completado, conforme indica a Figura 10, que se apresenta completa no Anexo C.

Figura 10 – Resultado do Ambiente 3

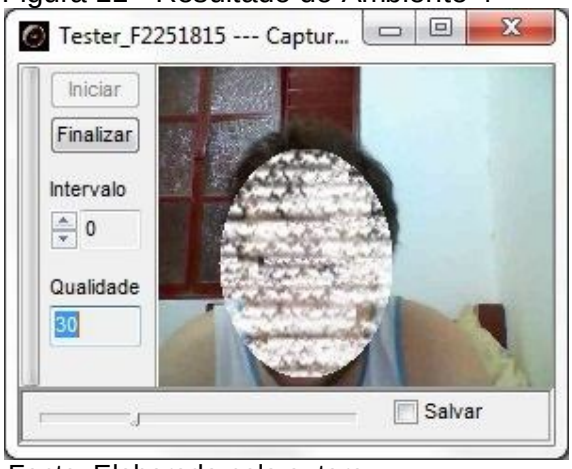


Fonte: Elaborado pela autora.

5.1.4 Ambiente 4

Nesse ambiente a máquina estava completamente desprotegida, ou seja, não estava com o firewall e nem com o antivírus ativos. Além do download do malware ter sido efetuado com sucesso, a conexão com a máquina invasora não foi bloqueada. Portando, nesse caso, a invasão foi bem sucedida, permitindo que a máquina invasora tivesse acesso remoto à máquina invadida através do software SpyNet, obtendo assim o controle da câmera da máquina, conforme mostrado na Figura 11 (imagem completa no Anexo D).

Figura 11 - Resultado do Ambiente 4

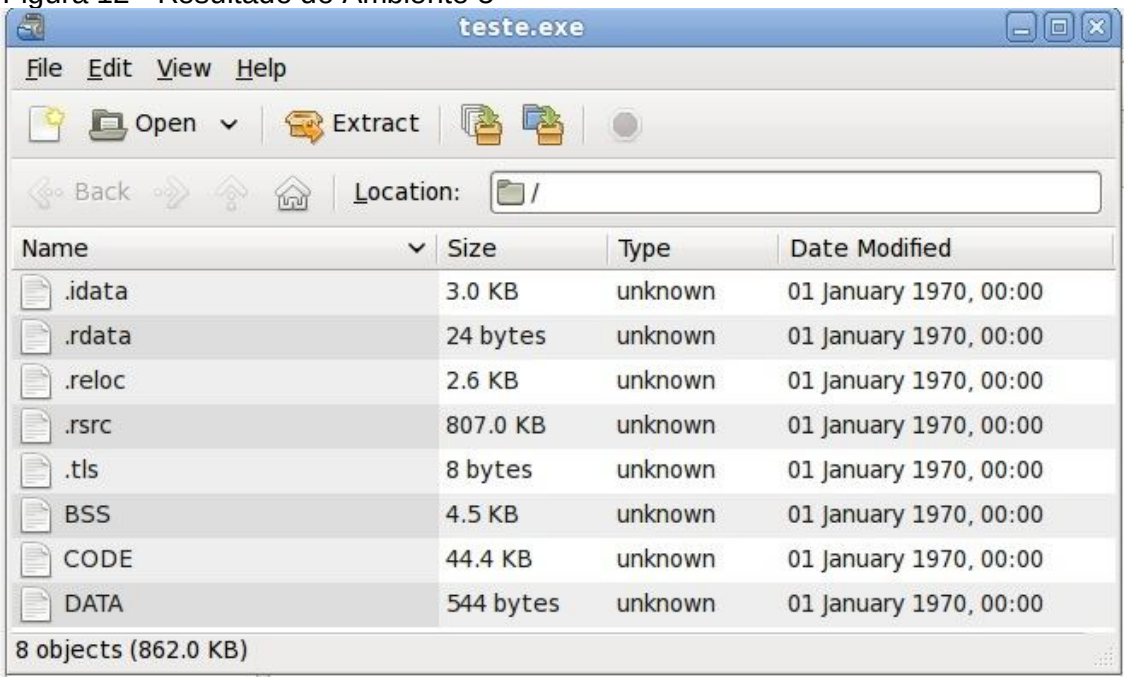


Fonte: Elaborado pela autora.

5.1.5 Ambiente 5

Nesse ambiente foi utilizado o sistema operacional Linux Tails. O arquivo foi baixado na máquina, mas como executáveis “rodam” apenas em Windows, tal arquivo não foi executado na máquina, assim a máquina não foi infectada, conforme mostra a Figura 12 (imagem completa no Anexo E).

Figura 12 - Resultado do Ambiente 5

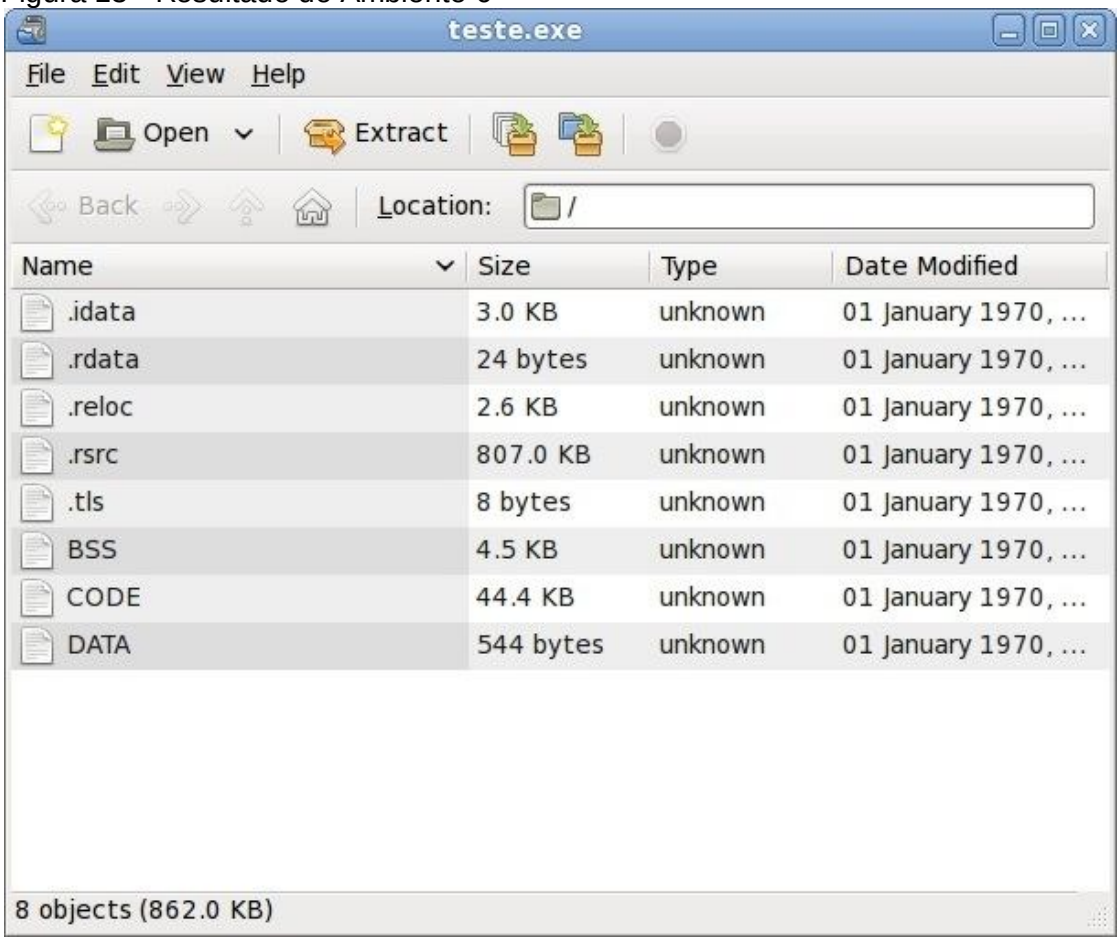


Fonte: Elaborado pela autora.

5.1.6 Ambiente 6

Nesse caso foi utilizada a máquina virtual com o sistema operacional Tails, e como no caso anterior, apesar do arquivo ter sido baixado na máquina, o mesmo não foi executado porque o arquivo só pode executado no sistema operacional Windows, conforme mostra a Figura 13 (imagem completa no Anexo F).

Figura 13 - Resultado do Ambiente 6



Fonte: Elaborado pela autora.

5.2 RESULTADO GERAL

Dos ambientes apresentados, em apenas um foi possível obter uma invasão bem sucedida, que foi o Ambiente 4, que está destacado na Figura 14 como o sucesso de invasão.

Figura 14 - Exibição do sucesso de invasão

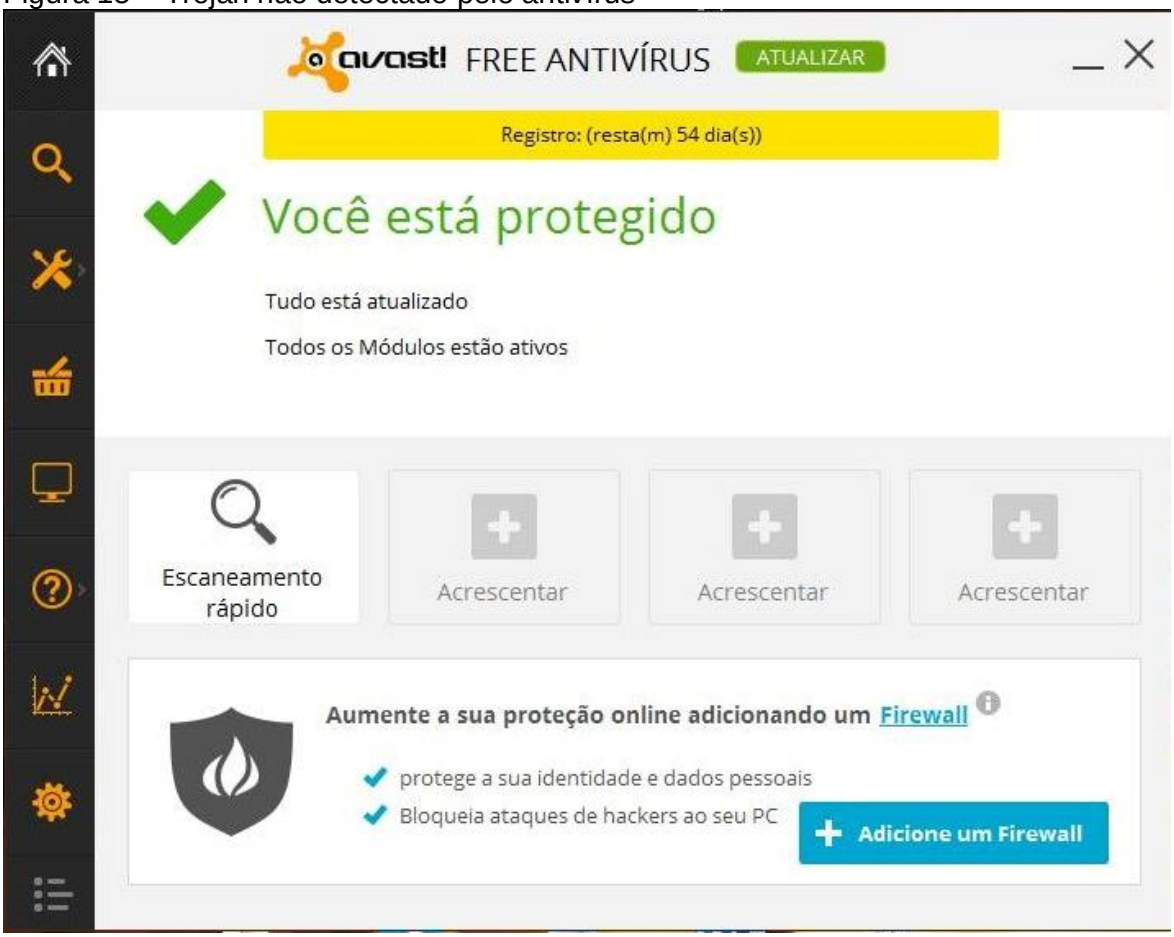
AMBIENTE	WINDOWS 7	TAILS	TOR	ANTIVIRUS	FIREWALL	MÁQUINA VIRTUAL
1	X		X	X	X	
2	X		X	X		
3	X		X		X	
4	X		X			
5		X	X			
6	X		X			X

Fonte: Elaborado pela autora.

Observa-se que é o único ambiente que tem o sistema operacional Windows e não possui nenhuma proteção ativa. Portanto, conclui-se que uma invasão tem mais chances de ser bem sucedida através da utilização de cavalos de troia se não houver nenhum sistema de defesa na máquina.

O antivírus foi ativado depois que a máquina estava infectada, e o antivírus mesmo assim não detectou nenhuma atividade suspeita na máquina conforme mostra a Figura 15, cuja imagem completa está no Anexo G.

Figura 15 – Trojan não detectado pelo antivírus



Fonte: Elaborado pela autora.

Portanto, mesmo com softwares que protegem a máquina, nem sempre pode-se garantir total segurança quando se trata de navegação na web.

Nos ambientes 5 e 6, ambos com sistema operacional Linux, não houve nenhuma chance de invasão pelo método utilizado porque o vírus foi desenvolvido especificamente para Windows.

O Linux é considerado um sistema operacional mais seguro que o Windows. Como já citado, o Windows foi criado em 1981, e em 1986 já havia registro de um vírus para o sistema operacional. (AZEVEDO, 2013). Já a primeira versão do Linux foi lançada em 1991, e em 2002 ainda não havia registro de um vírus criado para o mesmo. (BONAN, 2003). Portanto, vírus para Windows são produzidos a muito mais tempo que para Linux.

Outra dificuldade em desenvolver um vírus para Linux está nas permissões do administrador, o que torna o sistema mais seguro, pois o acesso às partes principais do sistema só acontece com senha. (SOARES; FERNANDES, 2013).

Uma das grandes diferenças entre o Windows e o Linux é que naquele o sistema decide qual arquivo é um programa através da extensão, enquanto nesse o que decide é a permissão, que é a opção “Permitir execução de arquivo como um programa”, que está presente nos arquivos do Linux. (MORIMOTO, 2009).

6 CONSIDERAÇÕES FINAIS

Um dos maiores receios das pessoas em navegar na Deep Web é o medo da infecção por vírus. Com a elaboração desse trabalho pode-se perceber que a forma mais segura de ser navegar na Deep web com o intuito de evitar ataques com malwares é utilizando o sistema operacional Linux, já que a maioria dos vírus para sistemas de ataques são voltados para o Windows. O motivo disso é que o Linux possui certas características que o tornam mais seguro.

Nota-se também que nem sempre um antivírus é eficiente, portanto o bom senso na busca de materiais na web torna-se o fator mais importante. Logo, navegar na Deep Web é muito semelhante a navegar na Surface Web, os cuidados a serem tomados devem ser exatamente os mesmos, como não sair clicando em todos os links que aparecem nas páginas, não abrir arquivos desconhecidos, não passar informações pessoais a estranhos, entre muitos outros cuidados que estamos acostumados a tomar para manter uma navegação segura.

As vantagens de se utilizar o Windows são os fatos de ele ser bastante intuitivo e a maioria dos usuários estarem acostumados com tal sistema operacional. Como a aparência do navegador Tor não é muito diferente dos navegadores convencionais, não é difícil se acostumar com o uso do mesmo, que pode ser utilizado para acessar sites que não sejam “.onion”. No entanto, a principal desvantagem de se utilizar o Windows é a sua vulnerabilidade a malwares, o que pode expor a identidade do usuário e ainda submetê-lo a outros riscos, como roubo de arquivos e informações pessoais.

A utilização do sistema operacional Linux em qualquer versão possui a vantagem de ser mais seguro contra ataques que usam malwares como técnica, mas não foi encontrada nenhuma desvantagem em utilizar o Linux Tails para utilização do Tor além do fato do mesmo não possuir uma interface tão agradável e de as pessoas estarem acostumadas com a do Windows. As demais desvantagens existentes na utilização do Linux para outras atividades não são relevantes para este trabalho.

Também foram feitas tentativas de acessos à contas de e-mail pessoal, mas chegou uma notificação ao e-mail vinculado à conta informando uma tentativa de acesso nos Estados Unidos, fato que confirma que o Tor oculta a verdadeira localização do usuário. Outras características que foram percebidas é o fato de que

cada vez que o Google é acessado com o Tor a página inicial é exibida com um idioma diferente e, quando é feita uma busca, os resultados obtidos ficam na língua em que a página inicial se encontra.

Utilizando a Hidden Wikki, a Google da Deep Web, foram encontrados muitos livros, artigos, filmes, e músicas que não foram possíveis ser localizadas na surface, o que prova que a Deep Web pode ter muito mais a oferecer que a Web.

Muito se fala em coisas de natureza criminosa na Deep Web como canibalismo, venda de drogas, armas e órgãos, mas como nada disso foi procurado, consequentemente não foi encontrado, portanto, só se encontra o que se procura. Logo, se a utilização da mesma é para pesquisas acadêmicas por exemplo, o material pesquisado será localizado, e não vídeos com cenas de violência, por exemplo.

Notou-se também que a discussão e o debate de temas que muitas vezes são evitados acontecem de maneira constante em fóruns ".onion", pois como a identidade é preservada as pessoas se sentem mais livres para tocarem em certos assuntos.

Conclui-se, portanto, que a Deep Web deve ser mais explorada e mais utilizada, como os adeptos ao movimento criptopunk defendem: a informação deve ser livre. E quanto mais pessoas utilizarem mais as falhas poderão ser corrigidas, porque assim será gerado mais conhecimento sobre o tema a ser compartilhado, explorado e debatido, podendo ser evitado que as coisas que são ilícitas continuem circulando em tal meio, e permitindo que as pessoas possam navegar na web sem medo de expor sua identidade e informações pessoais.

Uma limitação encontrada foi a dificuldade em se criar vírus pra Linux, que pode ser sugerido como trabalhos futuros a criação de um para elaboração de testes, bem como tentar com outros navegadores e outros sistemas operacionais. Podem ainda ser criados ambientes com outros antivírus e firewalls, gratuitos ou não, e a utilização de dispositivos móveis. Sugere-se ainda tentativas de invasão por outros métodos e outros tipos de vírus.

REFERÊNCIAS

A GUERRA dos navegadores. Produção e direção: Julian Jones. Oxford: Oxford Filmes Científicos para a Discovery Channel, 2008. (40 min).

ASSANGE, J. et al. **Cypherpunk**: liberdade e o futuro da internet. Tradução: Cristina Yamagani. São Paulo: Boitempo, 2013. Disponível em: <http://resistir.info/varios/assange_livro_port.pdf>. Acesso em: 01 mar. 2014.

AZEVEDO, R. M. R. **Propagação de Vírus Informáticos baseada em Modelos biológicos**. 2013. 67 f. Dissertação (Mestrado em Engenharia Informática, Área de Especialização em Arquitetura, Sistemas e Redes) - Instituto Superior de Engenharia do Porto, Porto, 2013. Disponível em : <https://dspace.isep.ipp.pt/jspui/bitstream/123456789/225/1/Tese_1090012_v1.pdf> Acesso em: 26 out. 2014

BERGMAN, M. K. The Deep Web: surfacing hidden value. **The Journal Of Electronic Publishing**, Ann Arbor, v. 7, n. 1, p. 1-17, ago. 2001. Disponível em: <http://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main>. Acesso em: 20 mar. 2014

BONAN, A. R. **Configurando e usando o sistema operacional Linux**. 2. ed. São Paulo: Futura, 2006.

CAMPOS, G. M. **Estatística para Prática para Docentes e Pós-Graduandos**, [1997?]. Disponível em: <http://www.forp.usp.br/restauradora/gmc/gmc_livro/gmc_livro_cap19.html>. Acesso em: 24 nov. 2014.

CHAUM, D. L. Untraceable electronic mail, return addresses, and digital pseudonyms**. Communications of the ACM**, New York, v. 24, n. 2, p. 84-90. fev. 1981. Disponível em: <http://dl.acm.org/citation.cfm?id=358563>. Acesso em: 10 mar. 2014.

CLARKE, I. et al. Freenet: a distributed anonymous information storage and retrieval system. In: INTERNATIONAL WORKSHOP ON DESIGNING PRIVACY ENHANCING TECHNOLOGIES: DESIGN ISSUES IN ANONYMITY AND UNOBSERVABILITY, 2000. Berkeley. **Anais...** Berkeley: [s.n.], 2000. p. 46-66. Disponível em: <http://dl.acm.org/citation.cfm?id=371977>. Acesso em: 10 mar. 2014.

_____. Protecting Free Expression Online with Freenet. **IEEE Internet Computing**, Nova York. v. 6, n. 1, p. 40-49. jan./fev. 2002. Disponível em: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=978368>. Acesso em: 10 mar. 2014.

COMER, D. E. **Interligação de Redes Com TCP/IP**. 5. ed. Rio de Janeiro: Campus, 2006. v.1.

DINGLEDINE, R.; MATHEWSON, N.; SYVERSON, P. Tor: the second-generation onion router. In: CONFERENCE ON USENIX SECURITY SYMPOSIUM, 13. 2004. San Diego, **Proceedings...** San Diego: [s. n.], 2004. p.1-17. Disponível em: <http://dl.acm.org/citation.cfm?id=1251396>. Acesso em: 10 mar. 2014

EGGER, C. et al. Practical Attacks Against the I2P Network. In: INTERNATIONAL SYMPOSIUM ON RESEARCH IN ATTACKS, 16. 2013. **Proceedings…** Santa Lucia: Intrusions and Defenses, 2013. Disponível em: <http://wwwcip.informatik.uni-erlangen.de/~spjsschl/i2p.pdf>. Acesso em: 02 mar. 2014.

EHLERT, M. **I2P Usability vs. Tor Usabilit**: A Bandwidth and Latency Comparison. Berlim: Universidade Humboldt, 2011. Disponível em: <http://userpage.fu-berlin.de/~semu/docs/2011_seminar_ehlert_i2p.pdf>. Acesso em: 02 mar. 2014

FEGAN, S. C.; FOROUZAN, B. A. **Protocolo TCP/IP**. 3. ed. Porto Alegre: MC Graw-Hill Interamericana, 2009.

GIL, A. C. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010.

GOLDSCHLAG ,D.; REEDY, M.; SYVERSON, P. Onion Routing for Anonymous and Private Internet Connections. **Communications of the ACM**, New York. v. 42, n. 2, p. 1-5. fev. 1999. Disponível em: <http://dl.acm.org/citation.cfm?id=293443&dl=ACM&coll=DL&CFID=350249830&CFTOKEN=22829137>. Acesso em: 10 mar. 2014.

_____. Hiding Routing Information.In: INTERNATIONAL WORKSHOP ON INFORMATION HIDING, 1. 1996. **Proceddings...** London: [s.n.], 1996. p. 137-150. Disponível em: <http://dl.acm.org/citation.cfm?id=731526>. Acesso em: 10 mar. 2014.

GRÉGIO, A. R. A. **Comportamento de programas maliciosos**. 2012. 156 f. Tese (Doutorado em Engenharia da Computação) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação, Campinas, 2012. Disponível em: <http://www.las.ic.unicamp.br/paulo/teses/20121128-PhD-Andre.Ricardo.Abed.Gregio-Malware.behavior.pdf>. Acesso em: 10 abr. 2014.

HADDOW, J. Será que precisamos nos esconder na internet?. **Vice**, 2012. Disponível em: <http://www.vice.com/pt_br/read/sera-que-precisamos-nos-esconder-na-internet>. Acesso em: 10 mar. 2014.

LAMARÃO, D. F.; MELONIO, G. V.; LAMARÃO, J. C. O. **Deep Web e o Sistema de Anonimato Tor**: Bitcoin. 2013. 60 f. Trabalho de Conclusão de Curso (Graduação em Redes de Computadores) - Faculdade de Tecnologia do Amapá, Macapá, 2013.

LEE, M. A Criptografia Funciona. **Fundação da Liberdade de Imprensa**, 2013. Disponível em: <https://pressfreedomfoundation.org/sites/default/files/criptografia_funciona.pdf>. Acesso em: 10 mar. 2014.

LOPES, A. Por trás das cortinas do computador. **O Estado RJ**, 2013. Disponível em: <http://www.oestadorj.com.br/mundo/por-tras-das-cortinas-do-computador/>. Acesso em: 10 mar. 2014.

MENEZES, A. J.; OORSCHOT, P. C. V.; VANSTONE, S.A. **Handbook of Applied Cryptography**. Nova York. CRC PRESS, 1996.

MORIMOTO, C.E. **Linux Guia Prático**. Porto Alegre: Sul Editores, 2009.

OLIVEIRA, W. **Técnicas para Hackers**: Solução para segurança. Versão 2. Coleção Tecnologias. Lisboa, Portugal: Centro Atlantico, 2003.

ONION Diagram. **Wikipedia**, 2008. Disponível em: <http://en.wikipedia.org/wiki/File:Onion_diagram.svg>. Acesso em: 10 mar. 2014.

POMPÉO, W. A. H.; SEEFELDT, J. P. Nem tudo está no Google: Deep Web e o Perigo da Invisibilidade. In: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 2. 2013. Santa Maria, **Anais…** Santa Maria: [s.n.], 2013. P. 439-449. Disponível em:<http://coral.ufsm.br/congressodireito/anais/2013/3-11.pdf>. Acesso em: 10 mar. 2014.

REALTIME Web Analytics With no Sampling. **Netmarketshare**, 2014. Disponível em: <http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0>. Acesso em: 10 mar. 2014.

SCHIMMER, L. Peer Profiling and Selection in the I2P Anonymous Network. In: PRIVACY ENHANCING TECHNOLOGIES CONVENTION, 4. 2009. **Anais...** Dresden: [s. n.], 2009. p. 59-70. Disponível em: <https://geti2p.net/_static/pdf/I2P-PET-CON-2009.1.pdf>. Acesso em: 10 mar. 2014.

SIKORSKI, M.; HONIG, A. **Pratical malware analysis**: the hands-on guide to dissecting malicious software. San Francisto: No Starch Press, 2012.

SILBERSCHATZ, A.; GALVIN, P. B.; GAGNE, G. **Fundamentos de Sistemas Operacionais**. 8. ed. Rio de Janeiro: LTC, 2010.

SILVA, P. T.; CARVALHO, H.; TORRES, C. B. **Segurança dos sistemas de informação**: Gestão estratégica da segurança empresarial. Lisboa, Portugal: Centro Atlantico, 2003.

SOARES,W; FERNANDES, G. **Linux Fundamentos**. São Paula: Érica, 2013.

SOBRE. **Tails**, [2014?]. Disponível em:<https://tails.boum.org/about/index.pt.html>. Acesso em: 10 mar. 2014.

STALLINGS, W. **Criptografia e Segurança de Redes**: Princípios e Práticas. 4. ed. São Paulo: Prentice-Hall, 2007.

SYVERSON, P. Brief selected history. **Onion Routing**, [2005?]. Disponível em: <http://www.onion-router.net/history.html>. Acesso em: 10 mar. 2014.

TANENBAUM, A. S. **Sistemas Operacionais Modernos**. 3. ed. São Paulo: Pearson Pretince Hall, 2010.

TESTE avalia os principais antivírus gratuitos. **Olhar Digital**, 2014. Disponível em: <http://olhardigital.uol.com.br/video/41644/41644>. Acesso em: 12 set. 2014

TOR: Overview. **TOR**, [2004?]. Disponível em: <https://tor.eff.org/about/overview.html.en>. Acesso em: 10 mar. 2014.

TOR security advisory: Old Tor Browser Bundles vulnerable. **TOR**, 2013. Disponível. em:<https://lists.torproject.org/pipermail/tor-announce/2013-August/000089.html>. Acesso em: 10 mar. 2014.

UMA HISTÓRIA do Windows. **Windows**, 2013. Disponível em: <http://windows.microsoft.com/pt-br/windows/history#t1=era0>. Acesso em: 10 mar. 2014.

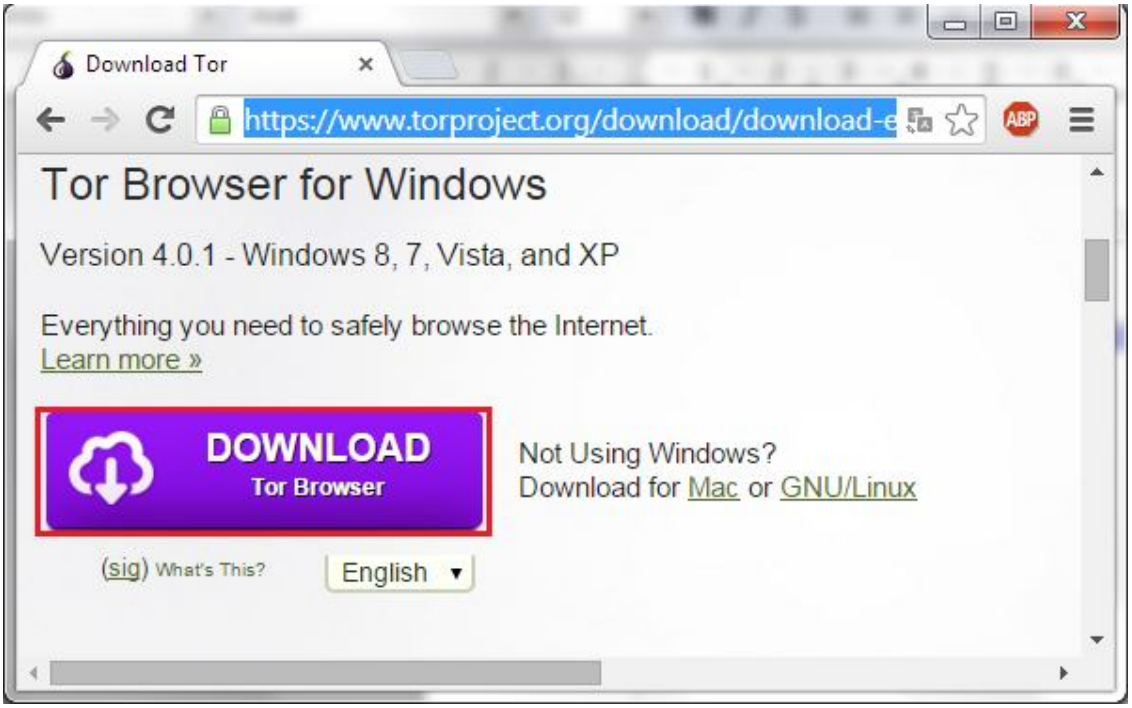
WETHERALL, D. J.; TANENBAUM, A. S. **Redes de Computadores**. 5. ed. São Paulo: Pearson Education, 2011.

ZELTSER, L.; SKOUDIS, E. **Malware**: Fighting Malicious Code. New Jersey: Prentice Hall, 2004.

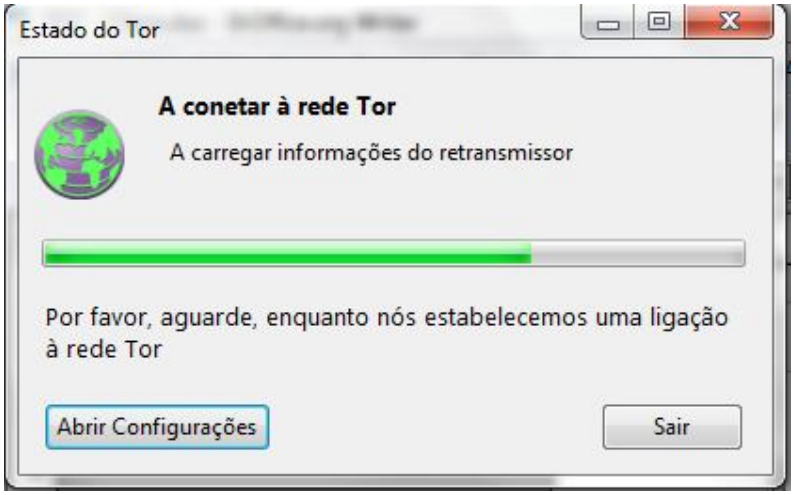
ZWICKY, E.; COOPER, S.; CHAPMAN, B. **Construindo Firewalls para Internet**. 2. ed. Rio de Janeiro: Campus, 2001.

APÊNDICE A – TUTORIAL DE INSTALAÇÃO DO TOR NO WINDOWS

Para utilização do Tor no Windows, abra o site https://www.torproject.org/download/download-easy.html.en e clique em Download:



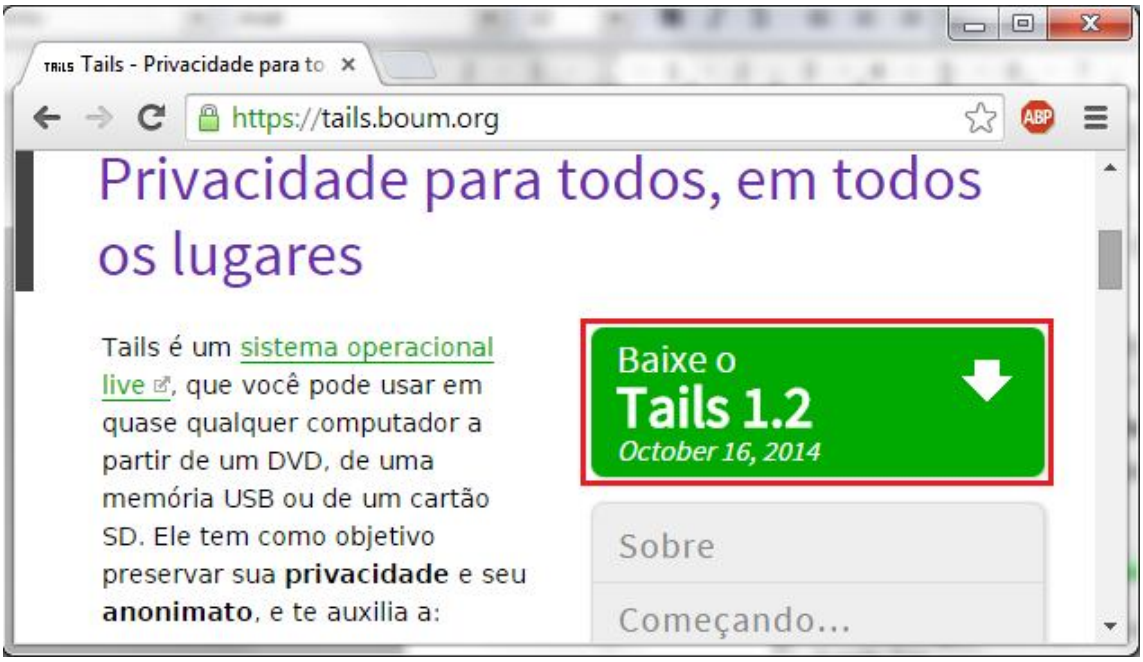
Execute o arquivo baixado. Será criada uma pasta na área de trabalho e haverá uma atalho chamado “Start Tor Browser”, dê um clique duplo e aparecerá uma janela de carregamento do Tor:



Quando finalizado, o navegador irá abrir.

APÊNDICE B – TUTORIAL DE INSTALAÇÃO DO LINUX TAILS

Para instalar o Tails no pendrive primeiro é necessário fazer o download da imagem iso. Para isso clique no link https://tails.boum.org/ e clique onde indica a figura abaixo:



Posteriormente clique no link http://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/ para fazer o donwload do arquivo que auxiliará a instalação do Tails no pendrive. Procure pelo ícone baixo para fazer o download:

Depois siga os passos descritos nos link https://tails.boum.org/doc/first_steps/installation/manual/windows/index.pt.html, que fica na página oficial do Tails.

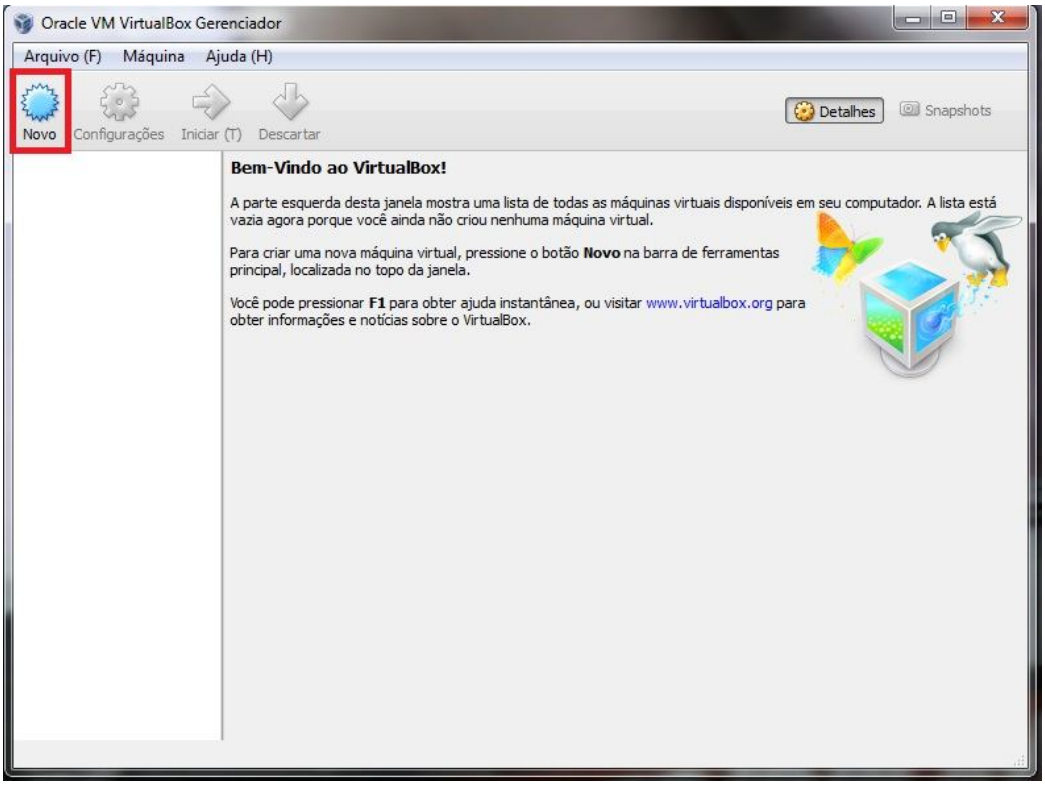
APÊNDICE C – TUTORIAL DE INSTALAÇÃO DA MÁQUINA VIRTUAL

Para criação de uma máquina virtual, acesse o link https://www.virtualbox.org/wiki/Downloads e faça o download do instalador clicando no link mostrado pela seta na figura abaixo:

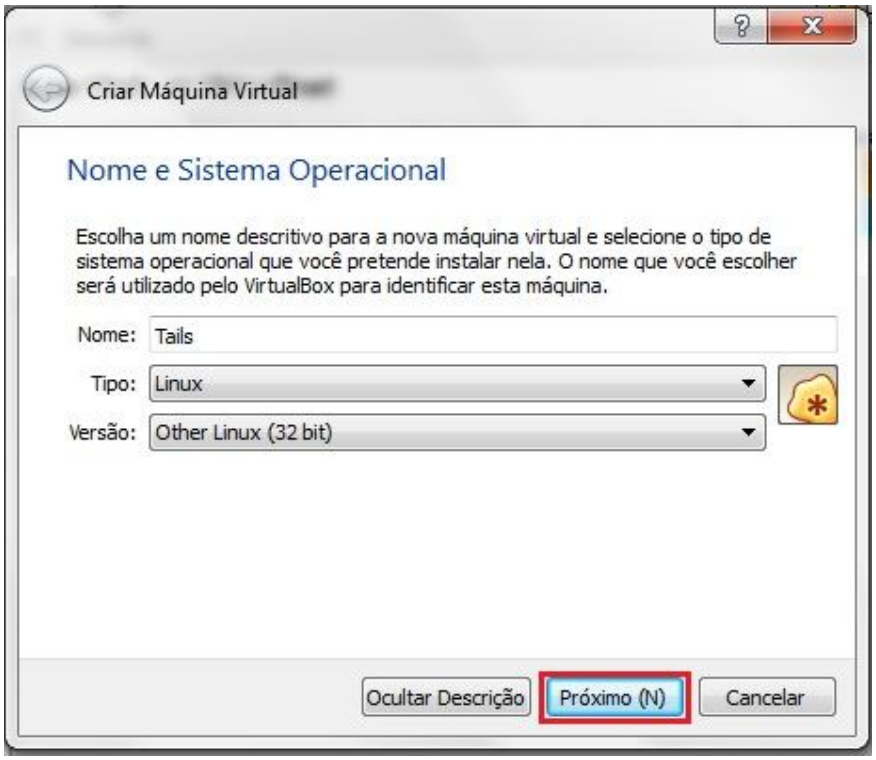
Execute e o instalador e vá clicando em next/próximo até finalizar a instalação. Se o Virtual Box não iniciar automaticamente, procure-o no Menu Iniciar e execute-o. Será necessário também o arquivo do tipo .iso, cujo download está explicado no Apêndice C.

Para criação da máquina virtual é necessário seguir os passos descritos nas figura que serão apresentadas, sempre clicando onde está marcado de vermelho.

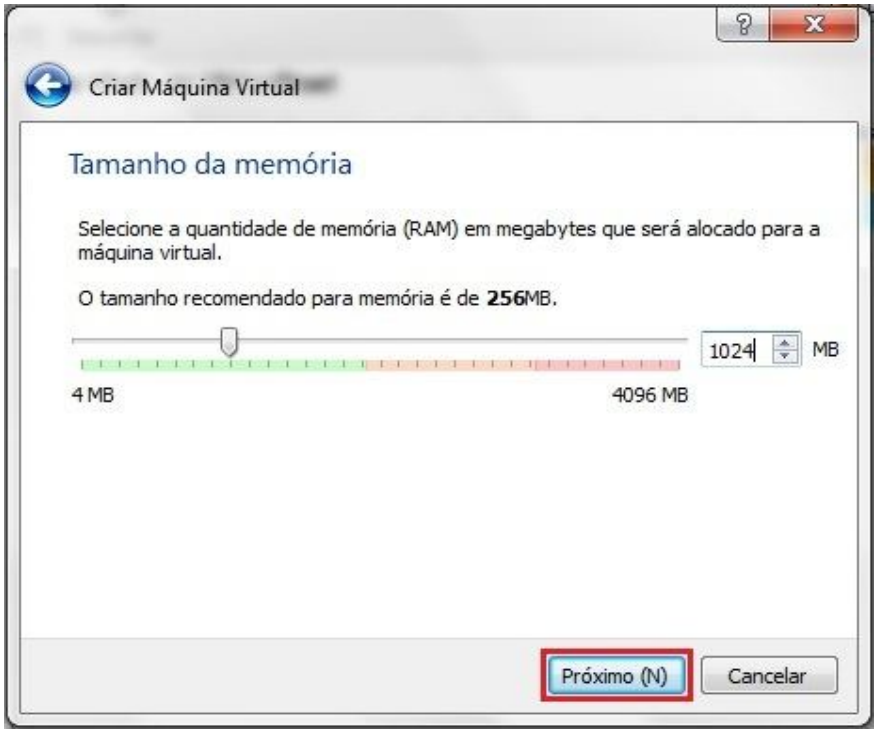
Para criar uma nova máquina, primeiramente é necessário clicar novo:



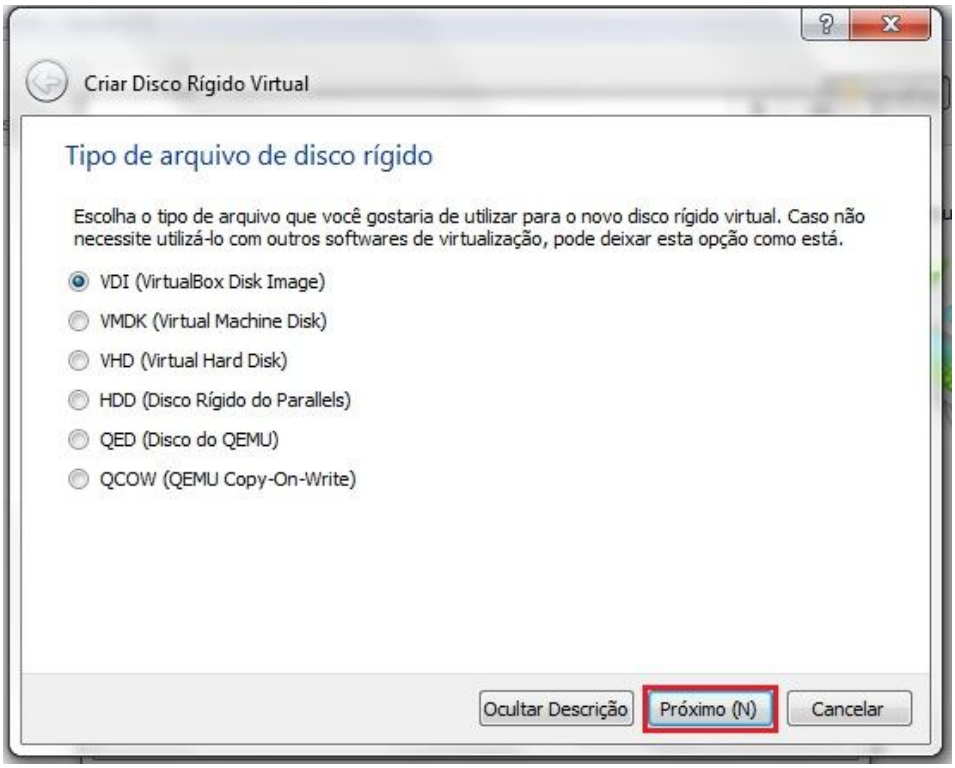
Preencha o nome e os campos descritos:

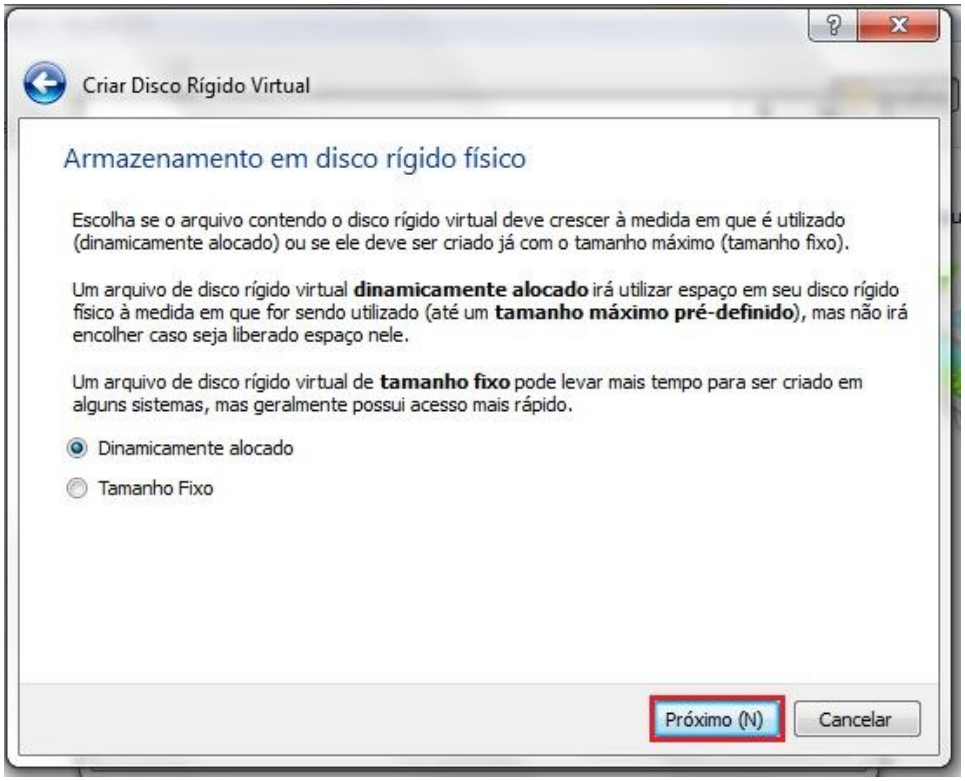


Selecione a opção 1024 MB:

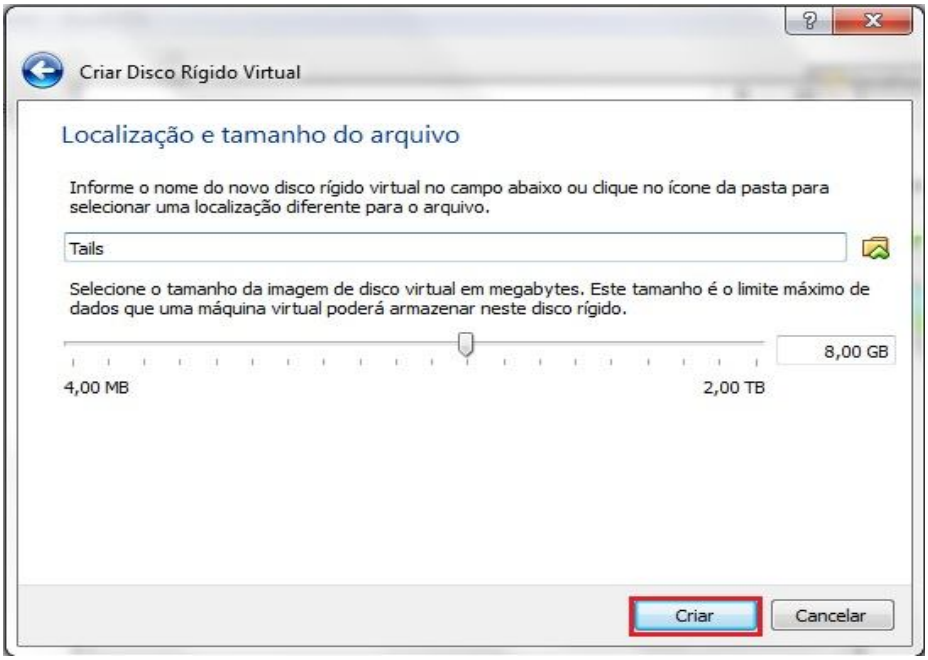


Selecione a segunda opção e clique em criar, e nas próximas duas janelas que abrirem clique em Próximo(N):

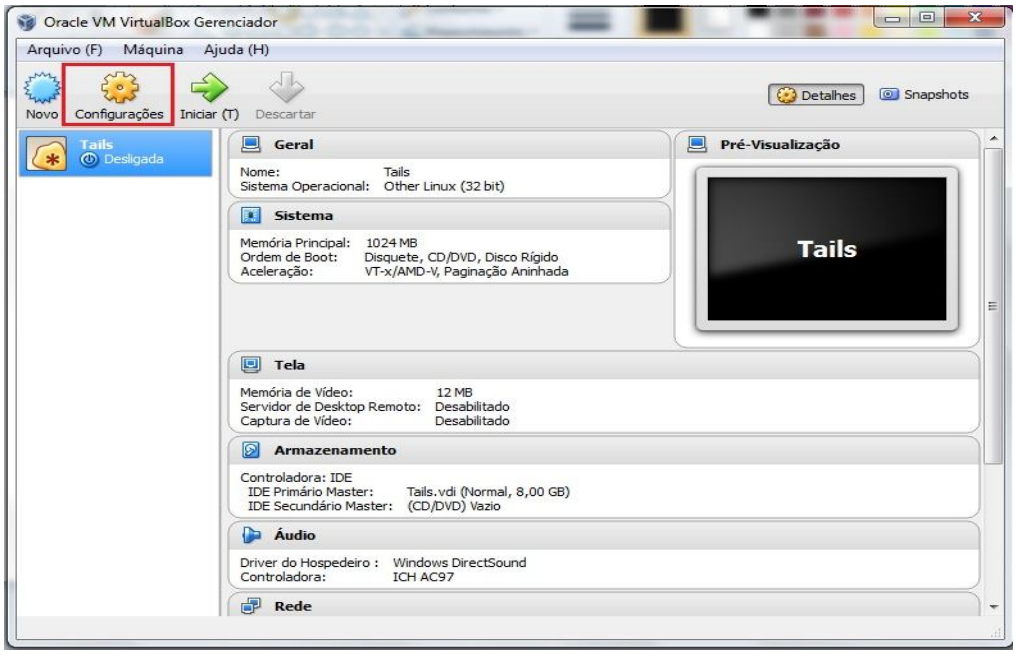

Criar Disco Rígido Virtual
Tipo de arquivo de disco rígido
Escolha o tipo de arquivo que você gostaria de utilizar para o novo disco rígido virtual. Caso não necessite utilizá-lo com outros softwares de virtualização, pode deixar esta opção como está.
VDI (VirtualBox Disk Image)
VMDK (Virtual Machine Disk)
VHD (Virtual Hard Disk)
HDD (Disco Rígido do Parallels)
QED (Disco do QEMU)
QCOW (QEMU Copy-On-Write)
Ocultar Descrição
Próximo (N)
Cancelar


Criar Disco Rígido Virtual
Armazenamento em disco rígido físico
Escolha se o arquivo contendo o disco rígido virtual deve crescer à medida em que é utilizado (dinamicamente alocado) ou se ele deve ser criado já com o tamanho máximo (tamanho fixo).
Um arquivo de disco rígido virtual dinamicamente alocado irá utilizar espaço em seu disco rígido físico à medida em que for sendo utilizado (até um tamanho máximo pré-definido), mas não irá encolher caso seja liberado espaço nele.
Um arquivo de disco rígido virtual de tamanho fixo pode levar mais tempo para ser criado em alguns sistemas, mas geralmente possui acesso mais rápido.
Dinamicamente alocado
Tamanho Fixo
Próximo (N)
Cancelar

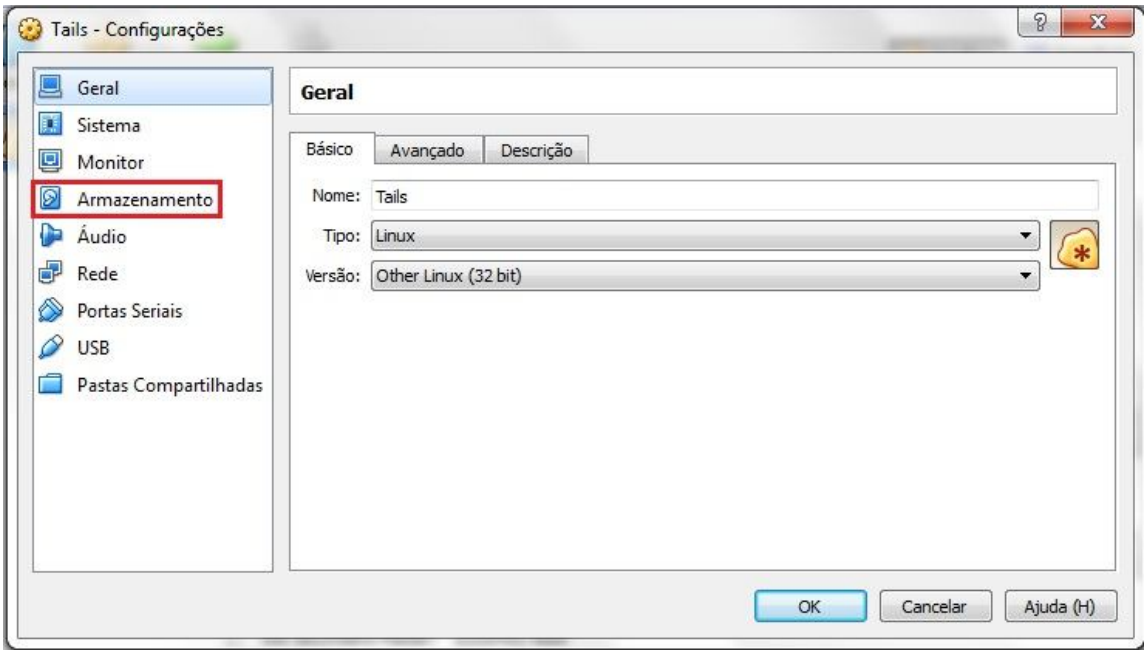
Até aqui foi feita apenas criação da máquina, mas ela ainda está vazia. Clique em criar:



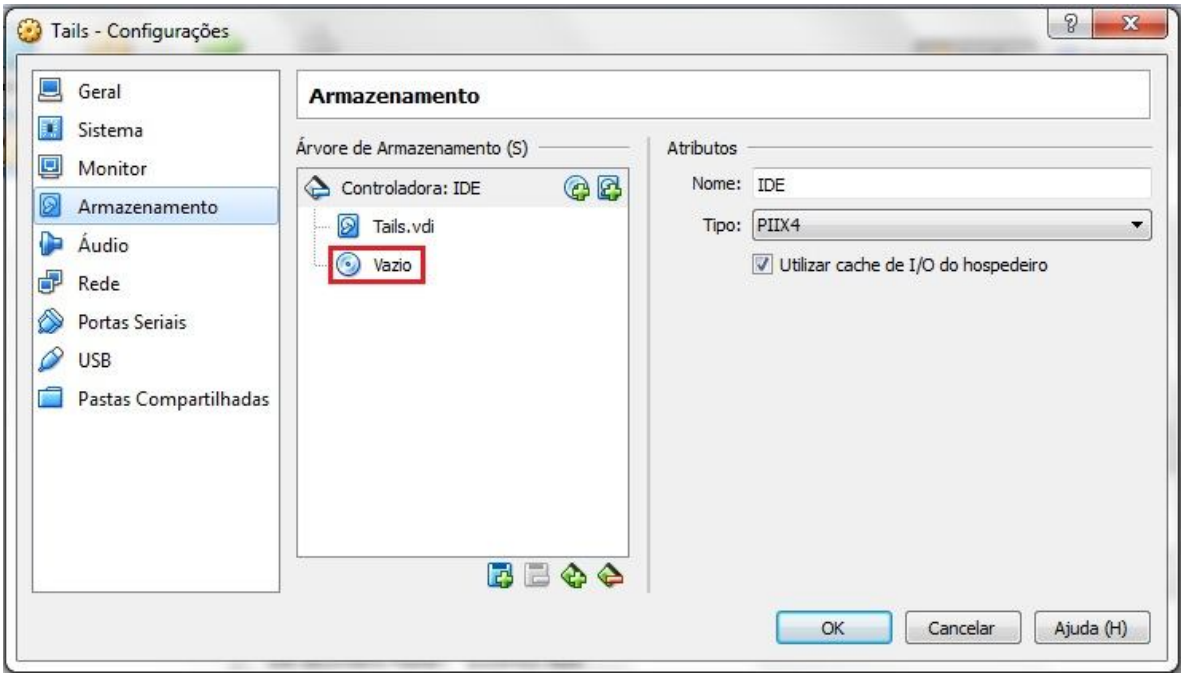
Agora o sistema operacional será colocado na máquina. Para início da configuração clique em configurações:



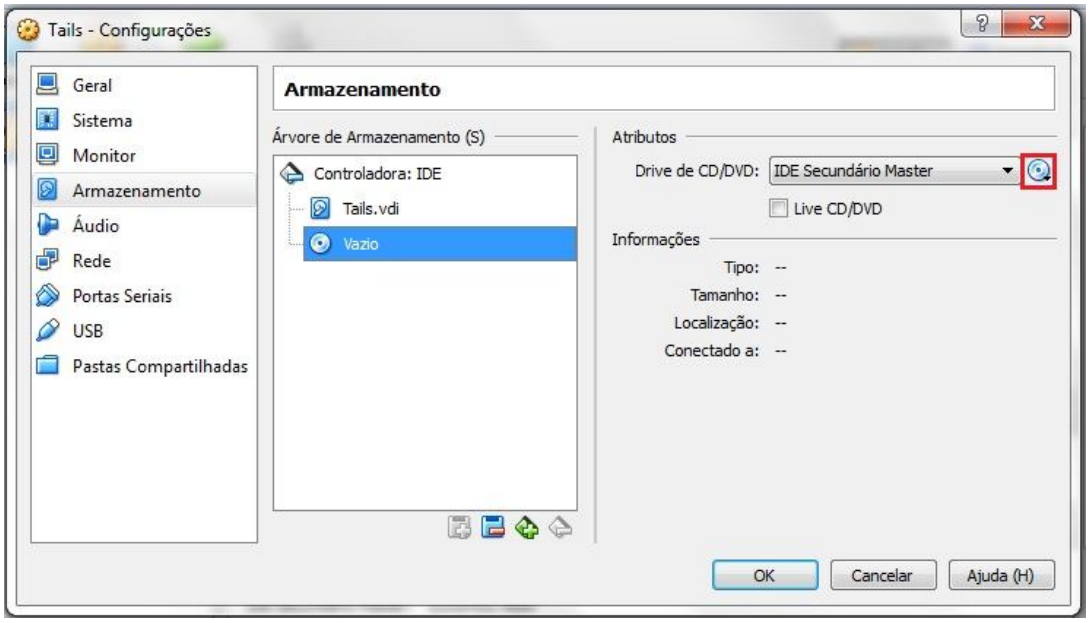
Irá abrir uma janela, clique na aba armazenamento:



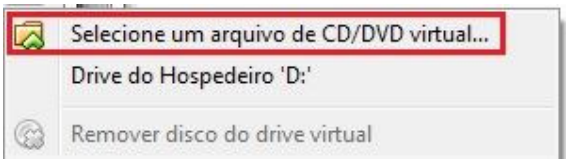
Clique no ícone representado por uma mídia óptica:



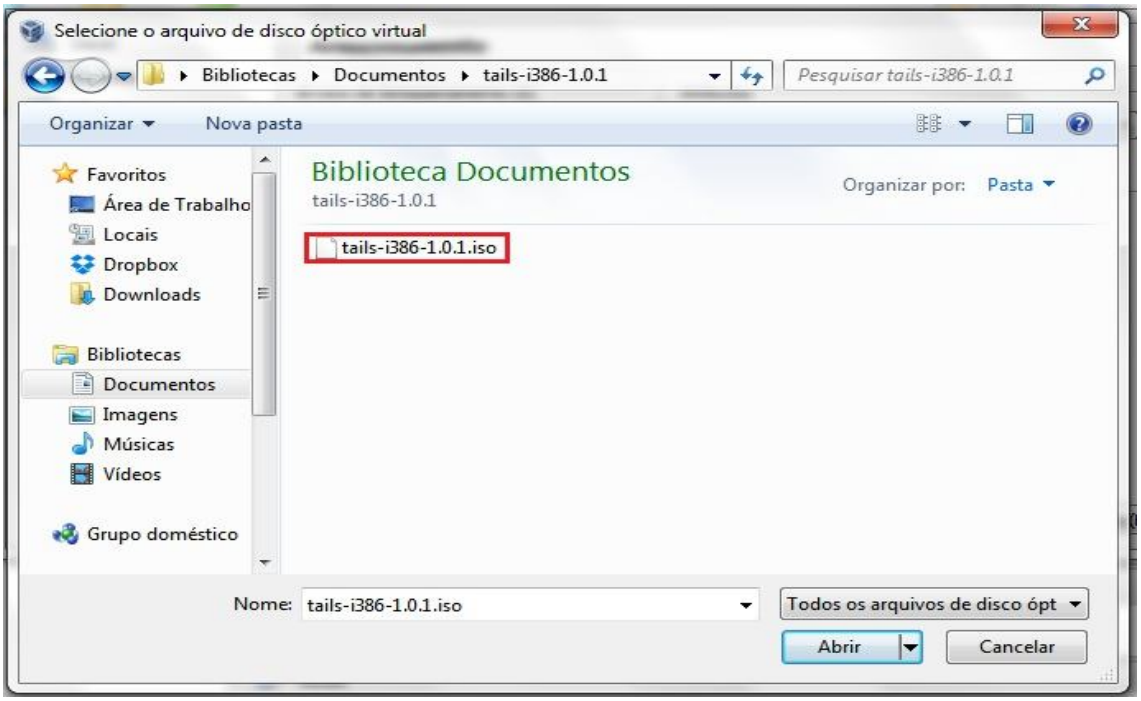
Irá abrir a opção na aba Atributos, no canto direito haverá outro ícone também representado por uma mídia óptica, clique nele:



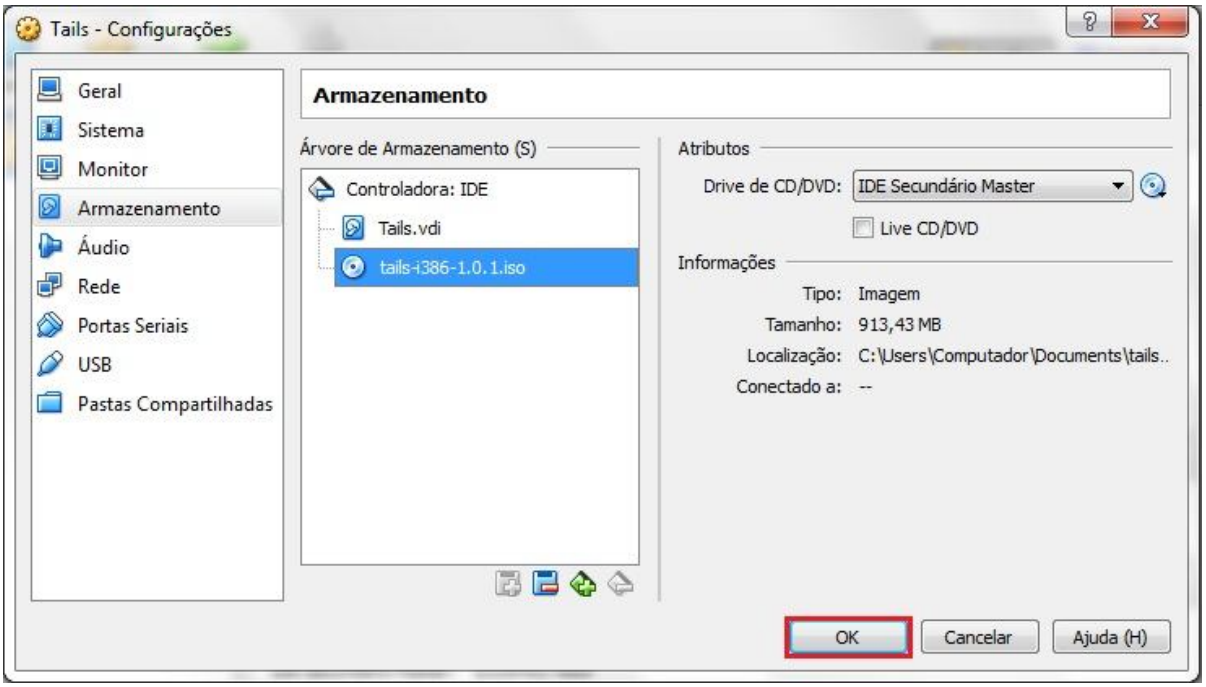
Irá abrir uma janela para que possa ser selecionado o sistema operacional a ser instalado, que é uma imagem, ou seja, um arquivo com a extensão .iso:



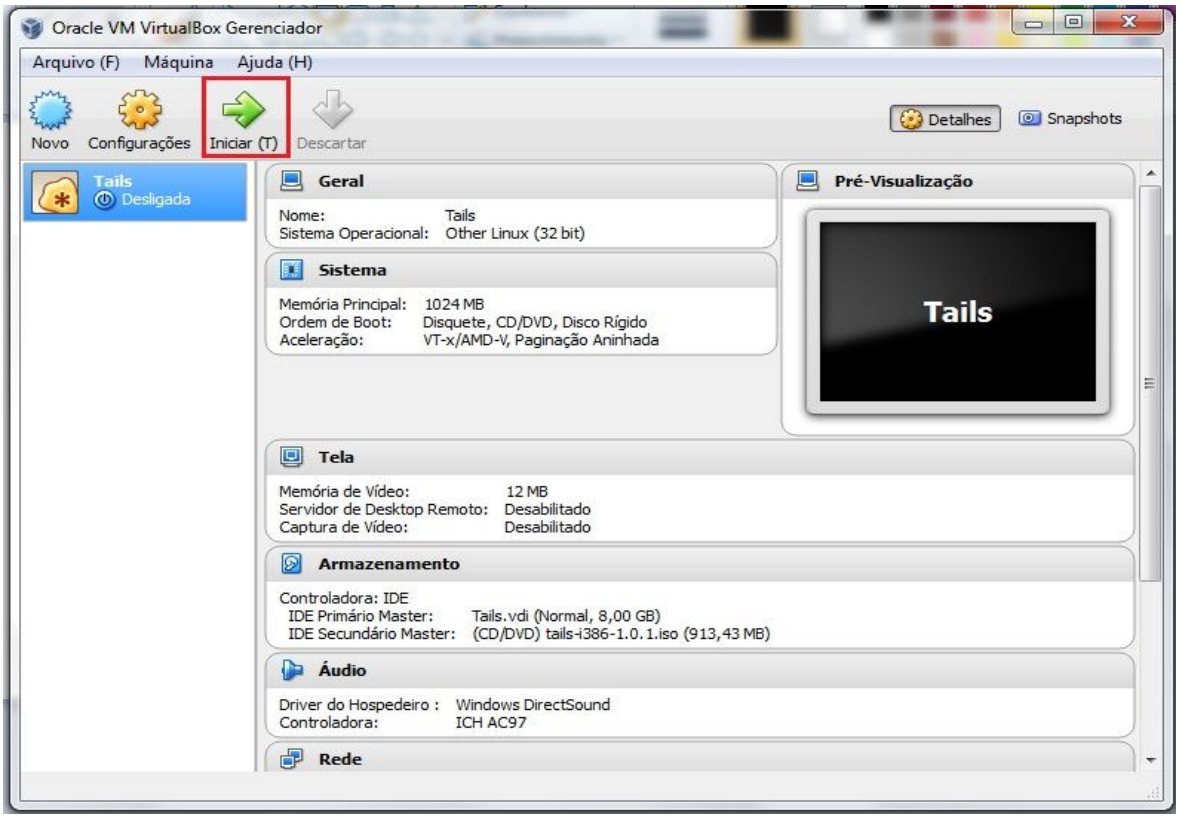
Abrirá uma janela para que seja localizado o arquivo, procure-o onde o mesmo foi armazenado no computador após a conclusão do download e selecione-o. Observe que no exemplo o arquivo foi armazenado na Biblioteca do Windows:



Observe como deve ficar e clique em ok:



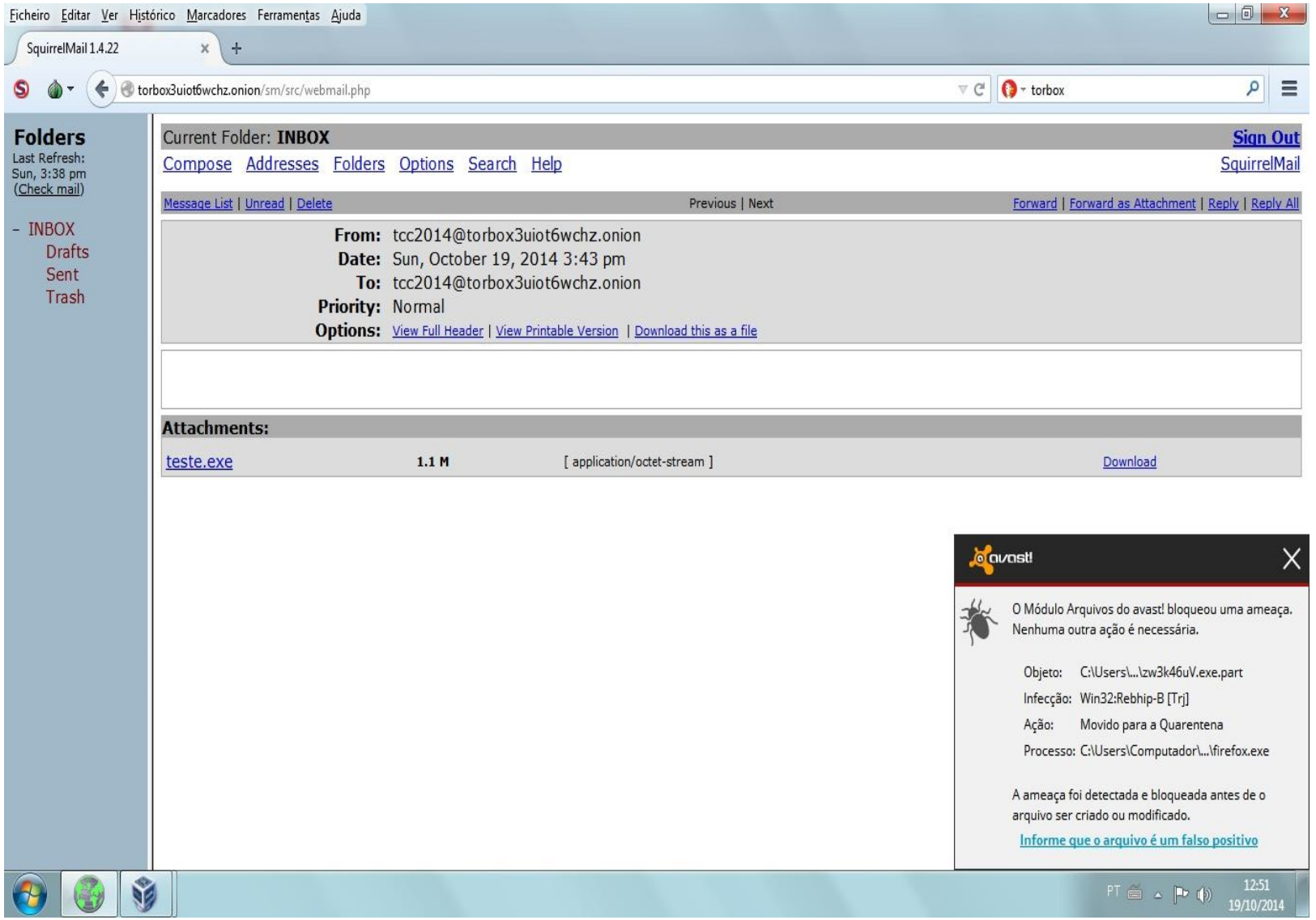
A janela fechará automaticamente. A máquina virtual com o sistema operacional Linux Tails está criada. Para inciá-la clique em Iniciar (T):



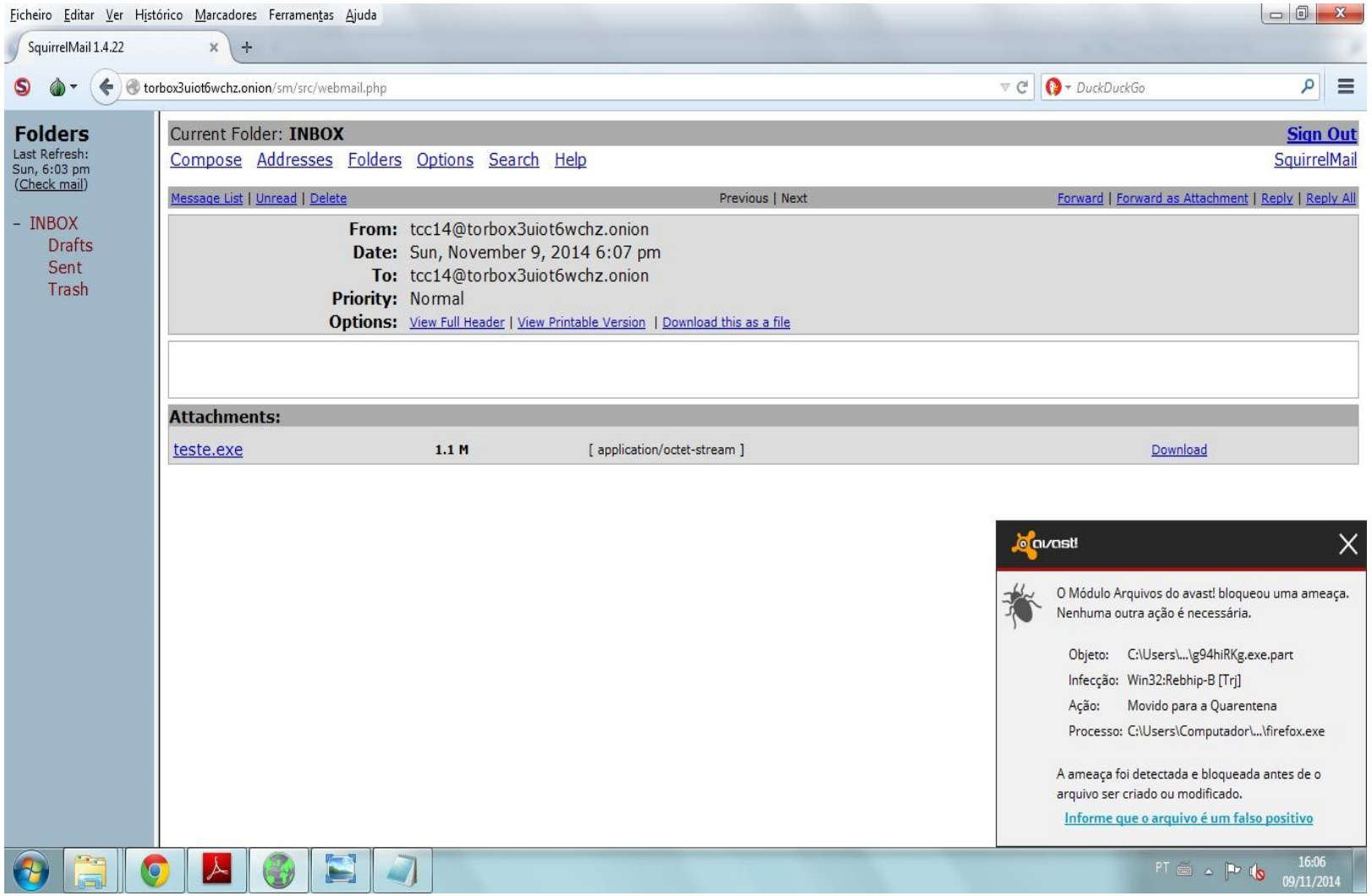
Após alguns segundos a máquina será iniciada, então clique em Login:

Agora a máquina está pronta para ser utilizada.

ANEXO A – FIGURA 8 COMPLETA

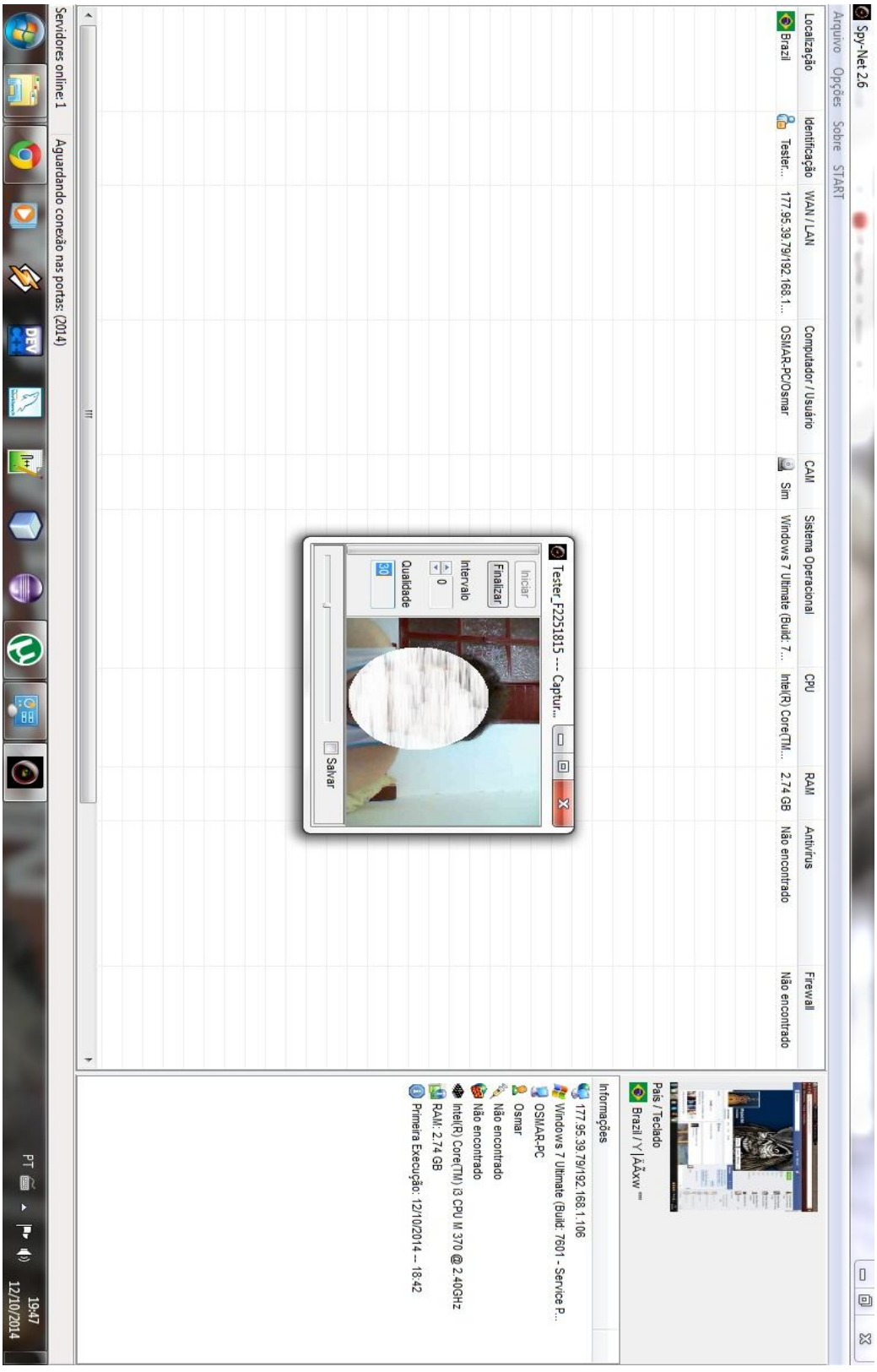


ANEXO B – FIGURA 9 COMPLETA

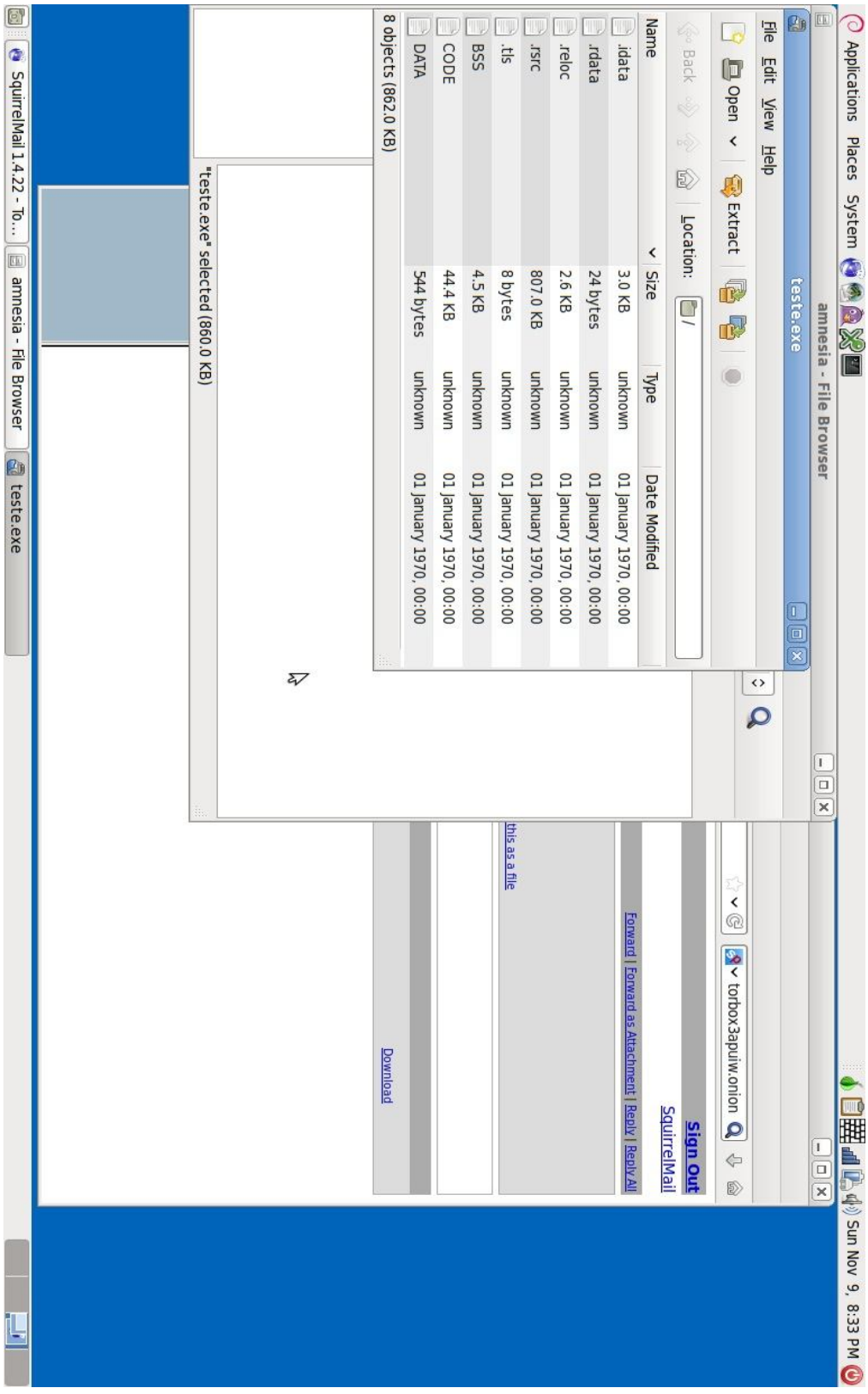


ANEXO C – FIGURA 10 COMPLETA

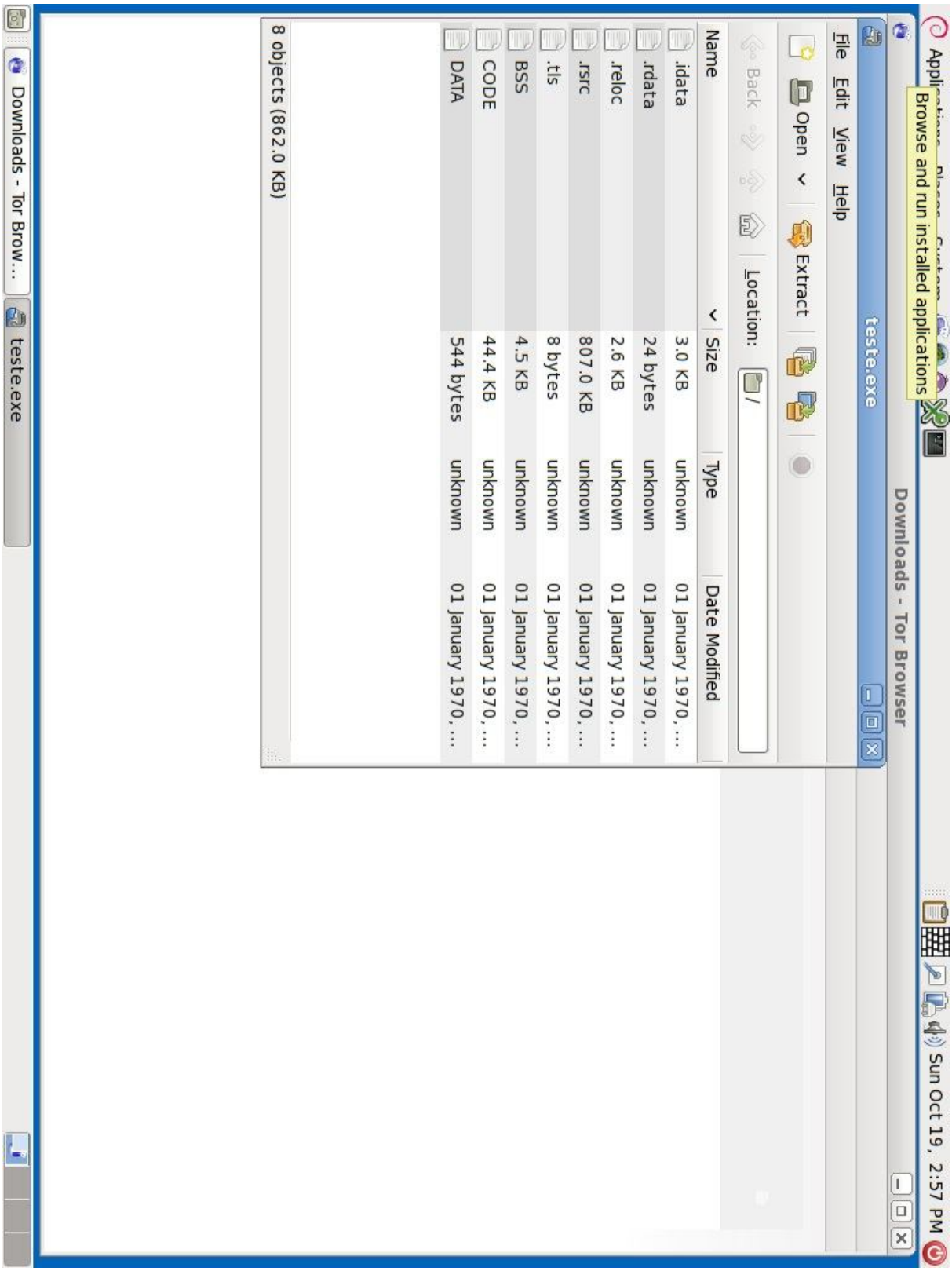
ANEXO D – FIGURA 11 COMPLETA



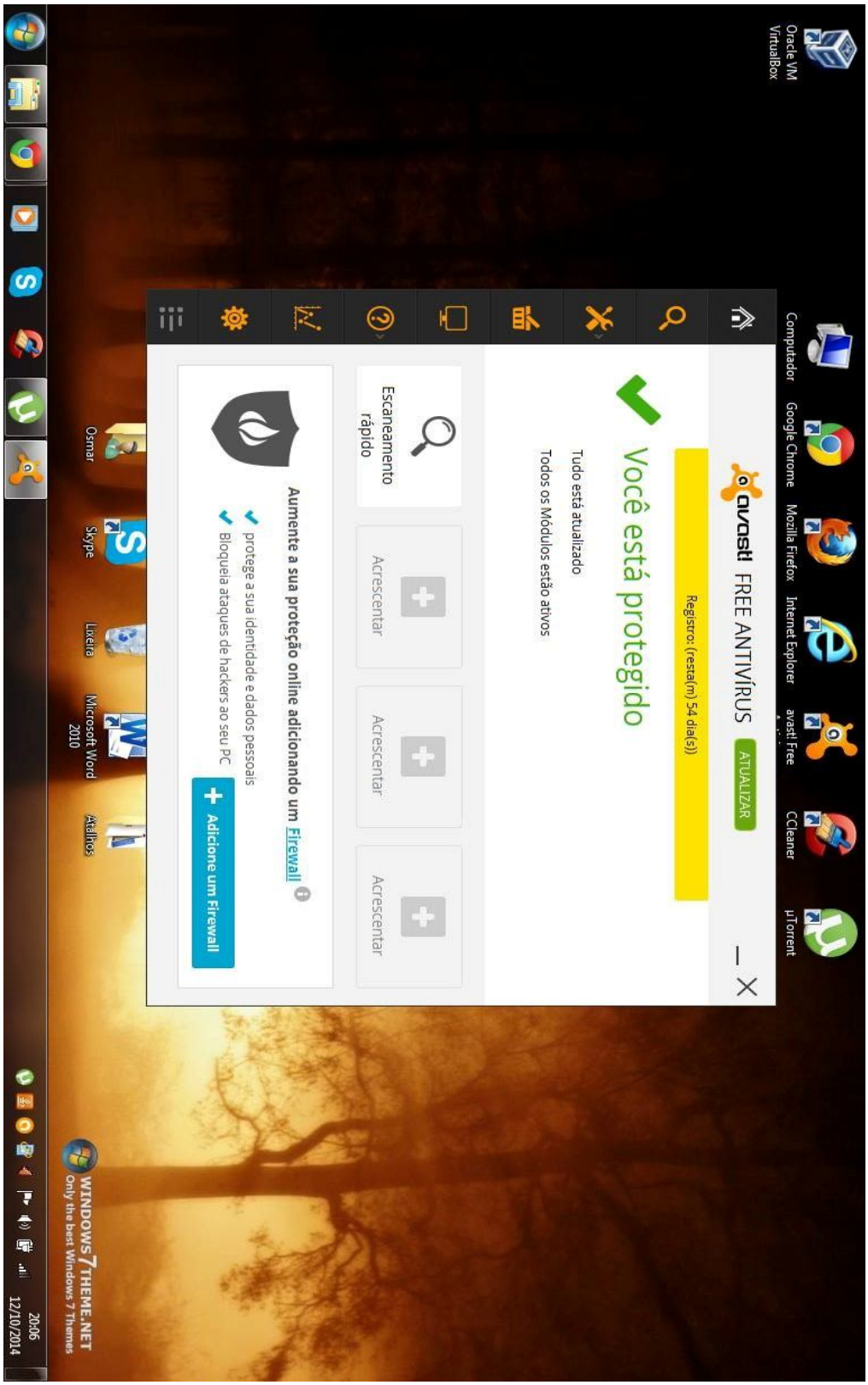
ANEXO E – FIGURA 12 COMPLETA



ANEXO F – FIGURA 13 COMPLETA



ANEXO G – FIGURA 15 COMPLETA



Um estudo da Deep Web e Análise das suas principais vulberabilidades

Danielle R. Líbano, Prof. Dr. Elvio G. Silva, Prof. Me. Patrick P. Silva, Prof. Me. Henrique P. Martins

Universidade Sagrado Coração (USC)
Caixa Postal 511 – 17.011-160 – Bauru – SP – Brasil

Abstract. *Deep Web is growing increasingly, but it is used illicitly and disapproved by society, which causes a lot of prejudice and fear of being utilized by other people. Be on the Deep Web means utilize anonymous navigation systems, in other words, protect the identity. Many people are not aware that is possible to use the internet anonymously, e even if they know, they`re too scared to use such resources due to the fame of the attacks and infections by virus on those who use such network. This work aims to know and analyze how a machine can be hacked so that can be possible to identify the best environment to utilize the Deep Web safely.*

Resumo. *A deep web vem crescendo cada vez mais, só que é utilizada de forma ilícita e desaprovada pela sociedade, o que causa muito preconceito e receio em ser utilizada por outros indivíduos. Estar na deep web significa utilizar sistemas de navegação anônima, ou seja, proteger a identidade. Muitas pessoas não sabem que é possível utilizar a internet anonimamente, e mesmo se sabem, têm medo de utilizar tais recursos devido à fama de ataques e infecções por vírus aos que utilizam tal rede. O desenvolvimento do trabalho visa conhecer e analisar como uma máquina pode ser invadida para que seja possível identifica o melhor ambiente para se utilizar a Deep Web com segurança.*

1. Deep Web

A Deep Web está ligada à internet, a diferença é que são utilizados túneis de comunicação diferentes para transferência de dados. Pelo fato das páginas não serem localizadas por provedores de busca comuns, seu conteúdo fica oculto na rede. Os usuários começaram a utilizá-la para fugir da vigia e monitoração, compartilhando informações e arquivos que não poderiam estar na internet comum. (BERGMAN, 2001).

As páginas da deep web não são indexadas aos motores de busca comuns, isso acontece propositalmente, ou porque o proprietário não quer que a página seja localizada ou porque a página não é estática.

Alguns dos motivos que levam as páginas a não serem indexadas são:

1. O fato de possuírem conteúdo privado sendo necessário uso de login e senha para evitar que informações sejam passadas para desconhecidos;
2. ou o dono da página optar pela privacidade, ou até mesmo, o conteúdo da mesma ser categorizado como conteúdo impróprio.

Para que o acesso a tal recurso seja bem sucedido, é necessário o uso de softwares específicos, como o Tor, por exemplo.

2. Tor (The Onion Router)

O Tor é um navegador específico para entrar na Deep Web, o qual utiliza o sistema de roteamento cebola, que é um sistema de encaminhamento de pacotes em uma rede de forma anônima. Nesse tráfego a conexão não ocorre diretamente com a máquina destino. Cria-se a comunicação utilizando uma cadeia de servidores proxy. (GOLDSCHLAG; REEDY; SYVERSON, 1999).

Antes das informações serem transmitidas, as mesmas são divididas em partes, onde cada uma recebe uma camada de criptografia no pacote a ser enviado, assim, cada Onion recebe uma chave para decifrar a mensagem até ser transformada em um texto simples. Para que esse texto chegue ao destino, todas essas camadas devem ser totalmente decifradas. Assim que o destino final é alcançado, uma resposta é transmitida ao solicitante. Quando a conexão é quebrada ou finalizada, todas as informações são eliminadas. É essa adição de camadas de criptografia que faz alusão à criação de uma cebola, também chamada de hop, e quando são descriptografadas diz-se que elas são descascadas. (DINGLEDINE; MATHEWSON; SYVERSON, 2004, tradução nossa).

No Tor, em vez da cebola ser gerada e descriptografada, suas chaves vão sendo geradas ao longo do tráfego. A rede Tor é formada por mais de 3600 servidores que atuam voluntariamente. A conexão passa por três nós antes de chegar ao seu destino final. (LEE, 2013).

3. Metodologia

De acordo com o funcionamento da Deep Web foram analisadas as vulnerabilidades dos riscos de ataques, aos quais os usuários estão expostos ao utilizar tal rede de comunicação. Foram feitos testes para descobrir em quais situações uma máquina pode ser invadida.

3.1 Configuração do ambiente

Para realizar a invasão foi utilizada uma máquina “invasora”, a qual dispõe das seguintes configurações: marca Dell com 4 GB de memória RAM, 500 TB de HD, com o sistema operacional Windows 7, onde foi configurado o software de invasão SpyNet e criado um vírus. A técnica utilizada para todas as tentativas de invasão foi o cavalo de troia. O tipo de invasão mais comum na internet é por meio de infecções, que acontece com malwares, dentre eles o mais conhecido e mais simples para realização de ataques é o cavalo de troia, sendo assim, o mais utilizado. O software SpyNet foi escolhido para elaboração do trabalho porque é simples e fácil de usar, podendo ser utilizado por qualquer pessoa que não tenha muitos conhecimentos na área de tecnologia da informação.

A máquina invadida possui as mesmas configurações que a citada anteriormente. No que diz respeito ao sistema operacional, o Windows 7 foi utilizado por ser atualmente o mais usado. (REALTIME, 2014).

Antes de começar a realização dos testes, foi feito um backup dos arquivos pessoais para evitar a perda de qualquer documento presente na máquina a ser atacada, e também foi feita uma limpeza os navegadores para eliminar senhas salvas evitando assim que a máquina utilizada para invasão ficasse vulnerável a outros invasores.

Primeiramente foi instalado o antivírus Avast, que foi escolhido por ser gratuito e também porque foi considerado um dos melhores antivírus gratuitos de 2014. (TESTE..., 2014). Como o Windows 7 já possui um firewall, não foi necessário a instalação de outro. Posteriormente foi preciso efetuar o download e instalação do Tor.

Esses foram os softwares necessários para os testes no Windows 7. Para utilização do Tails foi usado um pendrive da marca SanDisk de 8 GB, pois era necessário um pendrive de no mínimo 4 GB.

As duas últimas instalações foram do sistema operacional Linux Tails e da máquina virtual. Não foi necessário instalar o Tor no Tails, pois o mesmo já está presente no sistema operacional. Não foram utilizados antivírus para Tails devido à existência de poucos, bem como não haver muitas informações sobre eles, e o firewall do mesmo é embutido no próprio sistema.

No site oficial do Tor existe um comunicado explicitando a vulnerabilidade do Windows. (TOR, 2013). Portanto, o Tails foi escolhido para elaboração dos testes porque é um SO elaborado especificamente para preservar a identidade do usuário, servindo como complemento para o Tor, por exemplo. As especificações dos ambientes invadidos estão na Figura 1:

AMBIENTE	WINDOWS 7	TAILS	TOR	ANTIVÍRUS	FIREWALL	MÁQUINA VIRTUAL
1	X		X	X	X	
2	X		X	X		
3	X		X		X	
4	X		X			
5		X	X			
6	X		X			X

Figura 1 - Especificações dos Ambientes

Para invadir a máquina que é a suposta vítima, foi criada uma conta de email no TorBox. O mesmo possui extensão .onion, portanto só roda no Tor. Nessa conta foi anexado o trojan para que pudesse ser aberto e baixado na máquina a ser a atacada

3.2 Invasões

As invasões foram elaboradas conforme descrito anteriormente. Os resultados foram obtidos conforme segue.

3.2.1 Ambiente 1

Nesse primeiro ambiente a máquina com Windows 7 apresentava antivírus e firewall ativos. O Tor e o email foram abertos, e foi dado início ao download do arquivo.

3.2.2 Ambiente 2

As configurações do antivírus não foram alteradas, porém o firewall foi desativado pelo caminho “Botão Iniciar\Painel de Controle\Sistema e Segurança\Firewall do Windows\Personalizar Configurações”.

Como havia mais de uma rede, o firewall de todas elas foi desativado. O Tor foi fechado e aberto novamente, bem como o TorBox, então o download foi iniciado.

3.2.3 Ambiente 3

O antivírus foi desativado clicando na seta que fica no canto inferior direito da máquina "Mostrar ícones ocultos", posteriormente clicando com o botão direito do mouse sobre o ícone do Avast, então foi posicionada a seta do mouse sobre a opção "Controle dos módulos do Avast!" e foi selecionada a opção "Desabilitar até que o computador reinicie". O firewall foi reativado, pelo caminho Controle\Sistema e Segurança\Firewall do Windows\Personalizar Configurações. O Tor foi reiniciado e o TorBox foi aberto novamente, para então ser iniciado o download do arquivo novamente.

3.2.4 Ambiente 4

O antivírus foi mantido desativado, e o firewall foi desativado novamente conforme o caminho mostrado nas etapas anteriores. Novamente o Tor e o TorBox foram reiniciados, e o foi iniciado o download do arquivo mais uma vez.

3.2.5 Ambiente 5

Para ser utilizado o Tails, a máquina foi desligada, o pendrive no qual o sistema operacional estava instalado foi colocado na máquina. A máquina foi iniciada e o Linux Tails também. O Tor e o TorBox foram inicializados e o download do arquivo presente no email foi iniciado.

3.2.6 Ambiente 6

Para a máquina virtual foi utilizado o Oracle Virtual Box na sua versão mais recente, e então a máquina virtual Tails foi iniciada. Com o Tor e o TorBox carregados, foi realizado o download do arquivo.

4. Resultados

4.1 Ambiente 1

Nesse primeiro ambiente a máquina com Windows 7 estava com antivírus e firewall ativos. O email foi aberto, e foi dado início ao download do arquivo. Conforme mostra a Figura 2, o antivírus bloqueou o download do arquivo no navegador pois foi detectado que o arquivo era malicioso.

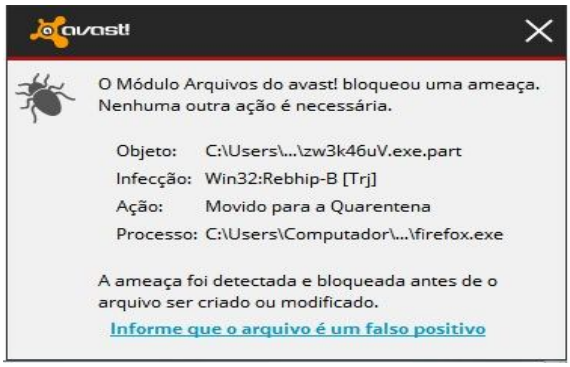


Figura 2 - Resultado do teste do Ambiente 1

4.2 Ambiente 2

Nesse caso a máquina estava apenas com o antivírus ativo, e assim como no ambiente anterior, o antivírus impediu que o arquivo malicioso fosse baixado, conforme mostra a Figura 3.

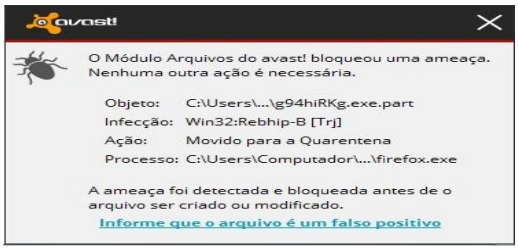


Figura 3 - Resultado do teste do Ambiente 2

4.3 Ambiente 3

Nesse caso apenas o firewall estava ativo, portanto o arquivo foi baixado e executado, mas o firewall detectou que seria feita uma conexão insegura, portanto bloqueou a finalização de execução do arquivo, impedindo que o ataque fosse completado, conforme indica a Figura 4.

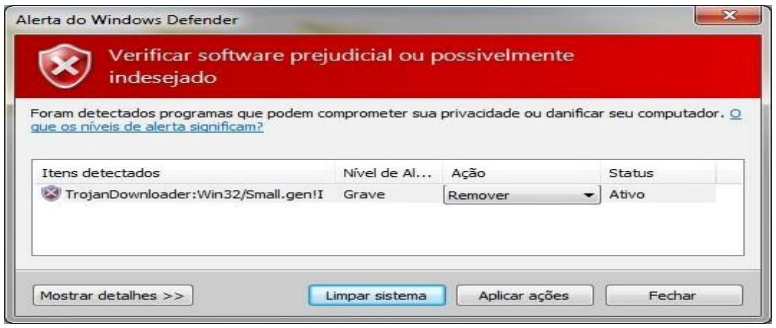


Figura 4 - Resultado do teste do Ambiente 3

4.4 Ambiente 4

Nesse ambiente a máquina estava completamente desprotegida, ou seja, não estava com o firewall nem com o antivírus ativos. Além do download do malware ter sido efetuado com sucesso, a conexão com a máquina invasora não foi bloqueada. Portando, nesse caso, a invasão foi bem sucedida, permitindo assim que a máquina invasora tivesse acesso remoto à máquina invadida através do software SpyNet, obtendo-se o controle da câmera da máquina, conforme mostrado na Figura 5.

Figura 5 - Resultado do teste do Ambiente 4

4.5 Ambiente 5

Nesse ambiente foi utilizado o sistema operacional Linux Tails. O arquivo foi baixado na máquina, mas como executáveis rodam apenas em Windows, tal arquivo não foi executado na máquina, assim a máquina não foi infectada, conforme mostra a Figura 6.

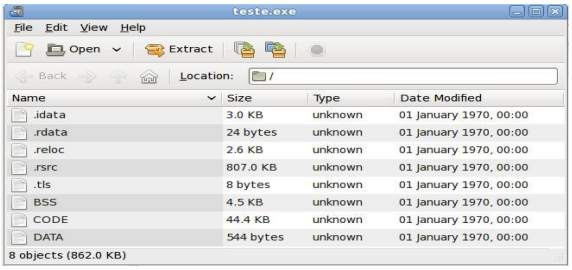


Figura 6 - Resultado do teste do Ambiente 5

4.6 Ambiente 6

Nesse caso foi utilizada a máquina virtual com o sistema operacional Tails, e como no caso anterior, apesar do arquivo ter sido baixado na máquina, o mesmo não foi executado, conforme mostra a Figura 7.

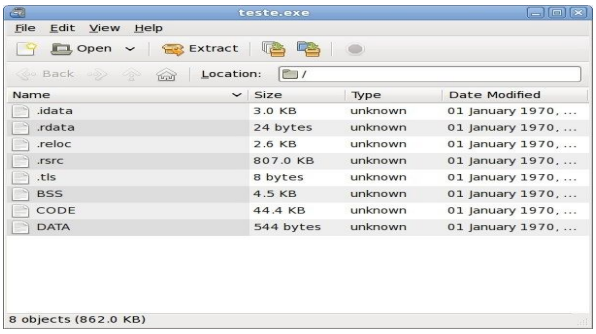


Figura 7 - Resultado do teste do Ambiente 6

5 RESULTADO GERAL

De acordo com os testes realizados, foi possível perceber que uma invasão só é bem sucedida através da utilização de cavalos de troia no sistema operacional Windows se não houver nenhum sistema de defesa na máquina, entretanto conforme mostra a Figura 8, o antivírus foi ativado depois que a máquina estava infectada, e o antivírus não detectou nenhuma atividade suspeita na máquina.

Figura 2 - Antivírus não detectou o malware

Nos ambientes 5 e 6, ambos com sistema operacional Linux, não houve nenhuma chance de invasão pelo método utilizado porque o vírus foi desenvolvido especificamente para Windows. O Linux é considerado um sistema operacional mais seguro que o Windows. Como já citado, o Windows foi criado em 1981, e em 1986 já havia registro de um vírus para o sistema operacional (AZEVEDO, 2013). Já a primeira versão do Linux foi lançada em 1991, e em 2002 ainda não havia registro de um vírus criado para o mesmo (BONAN, 2003). Portanto, vírus para Windows são produzidos a muito mais tempo que para Linux.

6 CONSIDERAÇÕES FINAIS

Um dos maiores receios das pessoas em navegar na Deep Web é o medo da infecção por vírus. Com a elaboração desse trabalho pode-se perceber que a forma mais segura de ser navegar na Deep web com o intuito de evitar ataques com malwares é utilizando o sistema operacional Linux, já que a maioria dos vírus para sistemas de ataques são voltados para o Windows.

Notou-se também que nem sempre um antivírus é eficiente, portanto o bom senso na busca de materiais na web torna-se o fator mais importante. Logo, navegar na Deep Web é muito semelhante a navegar na Surface Web, os cuidados a serem tomados devem ser exatamente os mesmos, como não sair clicando em todos os links que aparecem nas páginas, não abrir arquivos desconhecidos, não passar informações pessoais a estranhos, entre muitos outros cuidados que estamos acostumados a tomar para manter uma navegação segura.

As vantagens de se utilizar o Windows são os fatos de ele ser bastante intuitivo e a maioria dos usuários estarem acostumados com tal sistema operacional. Como a aparência do navegador Tor não é muito diferente dos navegadores convencionais, não é difícil se acostumar com o uso do mesmo, que pode ser utilizado para acessar sites que não sejam .onion. No entanto, a principal desvantagem de se utilizar o Windows é a sua vulnerabilidade a malwares, o que pode expor a identidade do usuário e submetê-lo a outros riscos, como roubo de arquivos e informações pessoais. A utilização do sistema operacional Linux em qualquer versão possui a vantagem de ser mais seguro contra ataques que usam malwares como técnica, mas não foi encontrada nenhuma desvantagem em utilizar o Linux Tails para uso do Tor, além do fato do mesmo não possuir uma interface tão agradável e que as pessoas estão acostumadas com a do Windows.

Também foram feitas tentativas de acessos à contas de email pessoal, mas chegou uma notificação ao email vinculado à conta informando uma tentativa de acesso nos Estados Unidos, fato que confirma que o Tor oculta a verdadeira localização do usuário. Outras características que foram percebidas foi o fato de que cada vez que o Google é acessado com o Tor a página inicial exibe um idioma diferente e, quando é feita uma busca, os resultados obtidos ficam na língua em que a página inicial se encontra. Utilizando a Hidden Wikki, a Google da Deep Web, foram encontrados muitos livros, artigos, filmes, e músicas que não foram ser localizadas na surface, o que prova que a Deep Web pode ter muito mais a oferecer que a Web. Muito se fala em coisas de natureza criminosa na Deep Web como canibalismo, venda de drogas, armas e órgãos, porém como nada disso foi procurado, e consequentemente não foi encontrado, portanto, só se encontra o que se procura.

Notou-se também que a discussão e o debate de temas que muitas vezes são evitados acontecem de maneira constante em fóruns .onion, pois como a identidade é preservada as pessoas se sentem mais livres para tocarem em certos assuntos.

Conclui-se portanto que a Deep Web deve ser mais explorada e mais utilizada, como os adeptos ao movimento criptopunk defendem: a informação deve ser livre. E quanto mais pessoas usarem mais as falhas poderão ser corrigidas, porque assim será gerado mais conhecimento sobre o tema a ser compartilhado, explorado e debatido, podendo ser evitado que as coisas que são ilícitas continuem circulando em tal meio, e permitindo que as pessoas possam navegar na web sem medo de expor sua identidade e informações pessoais.

Referências

AZEVEDO, R. M. R. **Propagação de Vírus Informáticos baseada em Modelos biológicos**. 2013. 67 f. Dissertação (Mestrado em Engenharia Informática, Área de Especialização em Arquitetura, Sistemas e Redes) - Instituto Superior de Engenharia do Porto, Porto, 2013. Disponível em : <https://dspace.isep.ipp.pt/jspui/bitstream/123456789/225/1/Tese_1090012_v1.pdf> Acesso em: 26 out. 2014

BONAN, A. R. **Configurando e usando o sistema operacional Linux**. 2. ed. São Paulo: Futura, 2006.

BERGMAN, M. K. The Deep Web: surfacing hidden value. **The Journal Of Electronic Publishing**, Ann Arbor, v. 7, n. 1, p. 1-17, ago. 2001. Disponível em: <http://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main>. Acesso em: 20 mar. 2014

DINGLEDINE, R.; MATHEWSON, N.; SYVERSON, P. Tor: the second-generation onion router. In: CONFERENCE ON USENIX SECURITY SYMPOSIUM, 13. 2004. San Diego, **Proceedings...** San Diego: [s. n.], 2004. p.1-17. Disponível em: <http://dl.acm.org/citation.cfm?id=1251396>. Acesso em: 10 mar. 2014

GOLDSCHLAG ,D.; REEDY, M.; SYVERSON, P. Onion Routing for Anonymous and Private Internet Connections. **Communications of the ACM**, New York. v. 42, n. 2, p. 1-5. fev. 1999. Disponível em: <http://dl.acm.org/citation.cfm?id=293443&dl=ACM&coll=DL&CFID=350249830&CFTOKEN=22829137>. Acesso em: 10 mar. 2014.

LEE, M. A Criptografia Funciona. **Fundação da Liberdade de Imprensa**, 2013. Disponível em: <https://pressfreedomfoundation.org/sites/default/files/criptografia_funciona.pdf>. Acesso em: 10 mar. 2014.

REALTIME Web Analytics With no Sampling. **Netmarketshare**, 2014. Disponível em: <http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0>. Acesso em: 10 mar. 2014.

TESTE AVALIA os principais antivírus gratuitos. **Olhar Digital**, 2014. Disponível em: <http://olhardigital.uol.com.br/video/41644/41644>. Acesso em: 12 set. 2014