CENTRO UNIVERSITÁRIO SAGRADO CORAÇÃO

Ana Carolina de Oliveira

CIBERATAQUES COM O RANSOMWARE EKANS E MECANISMOS DE DEFESA

BAURU
2022

Ana Carolina de Oliveira

CIBERATAQUES COM O RANSOMWARE EKANS E MECANISMOS DE DEFESA

Monografia de Iniciação Científica apresentado à Pró-Reitoria de Pesquisa e Pós-Graduação como parte dos pré-requisitos para aprovação do conselho, sob orientação do Prof. Me. Henrique Pachioni Martins.

BAURU
2022

Oliveira, Ana Carolina de

O48c

Ciberataques com o Ransomware Ekans e Mecanismos de Defesa / Ana Carolina de Oliveira. -- 2022.

54f. : il.

Orientador: Prof. M.e Henrique Pachioni Martins

Monografia (Iniciação Científica em Ciência da Computação) - Centro Universitário Sagrado Coração - UNISAGRADO - Bauru - SP

1. Segurança da Informação. 2. Ransomware. 3. Ekans. 4. Mecanismos de Defesa. I. Martins, Henrique Pachioni. II. Título.

Elaborado por Lidyane Silva Lima - CRB-8/9602

DEDICATÓRIA

Dedico este projeto de pesquisa totalmente a Deus, onde sem Ele eu não poderia ter chegado até aqui.

Aos meus amados familiares e amigos, onde em todo o processo me incentivaram a realizá-lo, e em todas as dificuldades enfrentá-las da melhor forma.

AGRADECIMENTOS

Agradeço ao meu professor e orientador, Henrique Pachioni Martins, por ter aceitado acompanhar-me neste, onde, com sabedoria e determinação me orientou durante a realização do projeto de pesquisa. O seu empenho foi essencial para a minha motivação à medida que as dificuldades iam surgindo ao período de realização.

RESUMO

A integração tecnológica é exponencial e coopera para melhorar diversas áreas do cotidiano da sociedade como um todo. Contudo, juntamente as facilidades, surgem grandes ameaças que colocam empresas e indivíduos em riscos. Baseando-se nisso, o objetivo desta pesquisa foi determinar como um dos mais recentes ransomwares descobertos, o Ekans, opera e de que forma os alvos podem se proteger da ameaça. Foi realizada uma tentativa de simulação de ataque utilizando máquinas virtuais, porém não foi possível por necessitar de maiores conhecimentos na linguagem de programação GO, redes de computadores e criptografia, entretanto baseando-se na pesquisa do INSIBE-CERT, foi possível verificar o funcionamento do ransomware Ekans e a identificação de melhores mecanismos de defesa.

Palavras chave: Segurança da Informação. Ransomware. Ekans. Mecanismos de Defesa.

ABSTRACT

Technological integration is exponential and cooperates to improve several areas of the daily life of society as a whole. However, along with the facilities, there are great threats that put companies and individuals at risk. Based on this, the purpose of this research was to determine how one of the most recent ransomware discovered, Ekans, operates and how targets can protect themselves from the threat. An attempt was made to simulate an attack using virtual machines, but it was not possible due to the need for more knowledge in the GO programming language, computer networks and cryptography. Ekans ransomware and the identification of better defense mechanisms.

Keywords: Information Security. Ransomware. Ekans. Defense Mechanisms.

SUMÁRIO

1. INTRODUÇÃO 9

2. OBJETIVOS 10

2.1. OBJETIVO GERAL 10

2.2. OBJETIVOS ESPECÍFICOS 10

3. REFERENCIAL TEÓRICO 10

3.1. SEGURANÇA DA INFORMAÇÃO 10

3.2. CIBERATAQUES 12

3.3. RANSOMWARE 13

3.4. MECANISMOS DE DEFESA 13

4. MATERIAIS E MÉTODOS 14

4.1. DESENVOLVIMENTO PRÁTICO 15

4.2. FERRAMENTAS UTILIZADAS – VIRTUALBOX E KALI LINUX 15

4.3. HARDWARE 16

5. RESULTADOS 16

5.1. CIBERATAQUES COM RANSOMWARE 16

5.1.1 CASOS DE CIBERATAQUES COM RANSOMWARE 17

5.2. MECANISMOS DE DEFESA CONTRA RANSOMWARE 18

5.3. CIBERATAQUES COM RANSOMWARE EKANS 19

5.3.1 CASOS CIBERATAQUES COM RANSOMWARE EKANS 19

5.4. SIMULAÇÕES DE ATAQUES 20

5.5. FUNCIONAMENTO DO RANSOMWARE EKANS 20

5.6. MECANISMOS DE DEFESA PARA O RANSOMWARE EKANS 22

6. DISCUSSÃO DOS RESULTADOS 23

7. CONSIDERAÇÕES FINAIS 23

8. REFERÊNCIAS 25

9. APENDICE 28

1. INTRODUÇÃO

A integração da computação na sociedade moderna se torna cada vez mais presente e cada vez mais profunda. Com isso várias novas possibilidades se tornam visíveis. Há inúmeras forma de usar o setor da Tecnologia da Informação para se maximizar lucros, automatizar tarefas cotidianas, gerenciar grandes quantidades de informações com uma eficiência jamais vista antes na história e entre outros. Em suma, é inegável que a tecnologia – de uma forma geral – trouxe grandes auxílios para a sociedade como um todo, no entanto, é igualmente inegável que junto a as novas possibilidades também vieram novas ameaças.

Assim como no mundo físico, o então nomeado “mundo virtual” possui ameaças tão perigosas – senão mais perigosas. Quanto mais integrado fica o mundo físico ao mundo virtual, maiores são as chances de um ciberataque ter efeitos gigantescos e prejudiciais, não somente a grandes empresas, mas também aos usuários dos sistemas de informação de forma geral.

Companhias multinacionais deixam a serviço da tecnologia processos de todos os escopos, desde serviços de contabilidade básicos, até linhas de produção inteiras. Obviamente, isso atrás – como já mencionado – grandes vantagens para as corporações, porém também as expõe a novos riscos. É possível hoje para linhas de montagem inteiras com algumas linhas de código; roubar dados confidenciais de funcionários, clientes, projetos; inutilizar servidores e entre outros.

Por esses motivos, as empresas precisam se preocupar e investir em tecnologias e politicas a fim de garantir a máxima segurança. Entre as tecnologias, estão os softwares de antivírus, chaves de criptografia, backups e etc. As políticas, por sua vez, consistem em normas de boas práticas para os funcionários, como regras de acesso à internet, acesso a recursos do sistema e etc.

De acordo com os dados fornecidos pelo site da CERT.br (Central de Estudos, Resposta e Tratamento de Incidente de Segurança no Brasil) a quantidade de ciberataques reportados em 2010 foi de 142.844 e em 2019 foi de

875.327, um aumento de aproximadamente 900% em menos de dez anos. Isso evidencia o impacto que esses ataques geram na sociedade como um todo. Por mais que alguns incidentes sejam “menores” e não tenham um escopo global, a relevância do tema não se perde. O mundo virtual ganha cada vez mais importância e cada vez mais espaço, se tornando cada vez mais fundamental e – consequentemente – perigoso.

2. OBJETIVOS

2.1. OBJETIVO GERAL

Explanar sobre o funcionamento do ransomware Ekans e constatar as melhores formas de defesa contra esse tipo de ciberataque.

2.2. OBJETIVOS ESPECÍFICOS

- Pesquisar sobre, ciberataques com ransomwares, mecanismos de defesas contra ransomwares e ciberataques com o ransomware Ekans;
- Verificar histórico de ciberataques com o ransomware Ekans;
- Determinar os principais tipos de alvos do ransomware Ekans;
- Identificar o modo como o ransomware opera;
- Constatar melhores mecanismos de defesa para o ransomware Ekans.

3. REFERENCIAL TEÓRICO

A seguir serão tratados alguns aspectos teóricos principais referentes a esta pesquisa.

3.1. SEGURANÇA DA INFORMAÇÃO

Aspirando-se que segundo o Dicionário Aurélio da Língua Portuguesa (2010, p. 689), entre as definições da palavra “segurança” há a “Estado, qualidade ou condição de seguro”, e, segundo o Dicionário Aurélio da Língua Portuguesa (2010, p. 426), entre as definições da palavra “informação” há a “Fatos conhecidos ou dados comunicados acerca de alguém ou algo”, portanto, pode-se concluir que segurança da informação consiste em proteger dados de indivíduos, empresas, governos e etc.

Atualmente, diversos sistemas são integrados e dependentes uns dos outros. Por isso é necessário que todas partes estejam seguras, já que o comprometimento de uma única parte, compromete o todo.

Existem cinco pilares básicos para a segurança da informação, sendo eles:

– Confidencialidade
– Integridade
– Disponibilidade
– Autenticidade
– Legalidade

Confidencialidade consiste no controle de acesso à informação apenas por aqueles que tenham permissão compatível com sua função, isto é, não deve existir acesso absoluto em um sistema. O acesso deve ser fragmentado de tal forma que não haja como um único individuo conhecer tudo.

Integridade se define como a garantia de que a informação será sempre completa e verdadeira, ou seja, sem que haja partes faltantes.

Disponibilidade, como o próprio nome sugere, é manter as informações sempre disponíveis de forma que estas nunca fiquem inacessíveis quando necessárias.

A autenticidade é a propriedade que assegura que toda informação está correta, em outras palavras, que não há falsificação.

Por fim, a legalidade define que toda a informação e toda e qualquer manipulação referente a ela, estará de acordo com a legislação determinada pelo país.

3.2. CIBERATAQUES

Pode-se definir ciberataques como a invasão de sistemas com o intuito de evidenciar, modificar, anular, destruir, ou roubar informações de empresas, pessoas, organizações, nações e etc. Os autores desse tipo de delito podem ser desde indivíduos únicos agindo de forma autônoma, até grupos, sociedades, organizações e nações.

De acordo com o CERT.br os ciberataques são feitos de várias formas, são eles:

- Worm: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- Dos (DoS -- Denial of Service): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- Invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede
- Web: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- Scan: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- Fraude: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem. (CERT.br, 2020).

O impacto de um ciberataque é sempre imprevisível. As consequências podem ser: um profundo abalo na reputação da empresa - por si só gera falta de confiança por parte dos investidores e perda de clientes; interrupção na

produção; exposições de informações sensíveis e aplicação de punições legais, como multas e prisões.

3.3. RANSOMWARE

Consolida-se ransomware como um software malicioso com a finalidade de bloquear os dados de um sistema, exigindo aos proprietários deste um pagamento para a recuperação das informações. Os primeiros ataques com ransomwares relatados ocorreram na Rússia no ano de 2005. Desde então, o esse modo operante de ataque se propagou pelo mundo.

Esse malware pode se instalar no sistema de diversas formas: través de sites maliciosos, links enviados por e-mail e redes sociais e instalação de aplicativos vulneráveis. Após a infecção o software pode bloquear a tela do computador e/ou tornar arquivos importantes inacessíveis por meio de criptografia.

No ano de 2013, por exemplo, houve um ataque de grande proporção atingindo diversas versões do sistema operacional Microsoft Windows causando danos a milhares de usuários e empresas.

A remoção de um ransomware é complexa, já que o acesso do usuário ao sistema foi comprometido. A melhor alternativa tanto para usuários pessoais, quanto para empresariais é a prevenção e utilização de mecanismos de defesa.

3.4. MECANISMOS DE DEFESA

> O único sistema verdadeiramente seguro é aquele que está desligado, desplugado, trancado num cofre de titanium, lacrado, enterrado em um bunker de concreto, envolto por gás nervoso e vigiado por guardas armados muito bem pagos. Mesmo assim, eu não apostaria minha vida nisso. (SPAFFORD).

Deste modo é possível verificar a importância dos mecanismos de defesa para proteger as informações, portanto é necessário, técnicas de defesa. Estas variam de acordo com a necessidade e o modelo do sistema dividindo-se em três categorias: física, administrativa e lógica.

A proteção física é referente a manutenção da integridade física (hardware) do sistema contra catástrofes naturais como incêndios, alagamentos, raios e entre outros. Como exemplo pode-se citar o sistema de refrigeração de um servidor. A função deste é a de manter os dispositivos sempre um uma temperatura favorável ao bom funcionamento, evitando a paralisação por superaquecimento.

A proteção administrativa refere-se à organização do núcleo da empresa, como por exemplo, selecionar a equipe responsável pela segurança.

A proteção lógica retrata o controle de acessos a informações. Um exemplo seria a utilização de usuários, senhas e níveis de acesso diferentes. Assim, pessoas externas não conseguem acesso nenhum aos dados e pessoas internas somente acessam os conteúdos que lhes são úteis para suas respectivas funções. Com abordagens como essa o rastreamento em casos de invasões, ou vazamento, também se torna uma tarefa mais simples, já que pelas informações vazadas é possível deduzir qual grupo de pessoas teria acesso a elas.

4. MATERIAIS E MÉTODOS

Pesquisas com propósitos acadêmicos propendem, em primeira instância, a deter o caráter de pesquisa exploratória, tendo em vista que raramente o pesquisador terá um conhecimento acerca do assunto retratado na pesquisa.

Segundo Gil (2010), as pesquisas exploratórias têm por finalidade proporcionar maior familiaridade com o problema, com o intuito de torná-lo mais explícito ou a construir hipóteses.

Á vista disso, este projeto trata-se de uma pesquisa exploratória com o objetivo é compreender como o ransomware Ekans opera. Usando para tal, simulações em máquinas virtuais. Como resultado, espera-se identificar os melhores mecanismos de defesa para esse ransomware.

O projeto será desenvolvido em duas etapas: na primeira foram realizadas pesquisas, estudos e desenvolvimento do embasamento teórico; na segunda serão feitos testes com a ferramenta VirtualBox com o objetivo de gerar conhecimento sobre os dados estudados.

Para o desenvolvimento do embasamento teórico e a descrição das atividades, houve a necessidade de realizar pesquisas sobre:

a) Conceituação de segurança da informação;
b) Conceitos e casos de ciberataques;
c) Características de ransomwares;
d) Conceitos de mecanismos de defesa;
e) Características e funcionamento da ferramenta de virtualização de máquinas VirtualBox;
f) Testes com a ferramenta VirtualBox para simulação de ciberataques com o ransomware Ekans;
g) Identificação de melhores mecanismos de defesa.

4.1. DESENVOLVIMENTO PRÁTICO

Foram feitas simulações utilizando duas máquinas virtuais sendo uma a atacante e outra o alvo. A máquina atacante teve como sistema operacional o Kali Linux enquanto a máquina alvo teve instalado o sistema operacional Microsoft Windows 10 Home.

A atacante usou o ransomware Ekans e realizou ataques a máquina alvo. Com os resultados obtidos pela máquina alvo foi analisado o comportamento do ransomware. Com a análise concluída, identificou-se os melhores mecanismos de defesas contra a ameaça.

4.2. FERRAMENTAS UTILIZADAS – VIRTUALBOX E KALI LINUX

> O Oracle VM VirtualBox, software de virtualização de plataforma cruzada de código aberto mais popular do mundo, permite que os desenvolvedores forneçam código mais rápido executando vários sistemas operacionais em um único dispositivo. (ORACLE).

“Kali Linux é uma distribuição Linux [...] de código aberto voltada para várias tarefas de segurança da informação, como teste de penetração, pesquisa

de segurança, computação forense e engenharia reversa.” (KALI LINUX, tradução nossa).

A escolha da ferramenta VirtualBox deveu-se a:

a) Ser uma ferramenta de código aberto.
b) Possibilidade de utilização de mais de uma máquina virtual ao mesmo tempo.
c) Possibilidade de usar sistemas operacionais diferentes.
d) Ser de conhecimento prévio da pesquisadora.

A escolha do sistema operacional Kali Linux deveu-se a:

a) Possuir código aberto.
b) Possuir ferramentas nativas que auxiliam na simulação de invasão.
e) Ser de conhecimento prévio da pesquisadora.

4.3. HARDWARE

O projeto foi desenvolvido utilizando como principal ferramenta um computador pessoal (PC), com o sistema operacional Windows 10 Pro – 64 bits, processador Intel® Core™ i5 CPU 650 @ 3.20GHz com memória RAM de 4 GB. O fundamento da escolha do computador se deve pela razão de pertencer à pesquisadora, além de, em primeiro momento, suprir as necessidades da pesquisa.

5. RESULTADOS

5.1. CIBERATAQUES COM RANSOMWARE

O Ransomware é um software malicioso que utiliza da criptografia para tornar inacessíveis arquivos ou/e documentos, geralmente esses arquivos fazem parte de uma rede ou servidor e para que se obtenha novamente esses arquivos íntegros novamente e não haja o vazamento ou deleção desses dados é exigido um pagamento.

Para infectar as máquinas são utilizadas diversos meios como phishing, que são e-mails ou mensagens com links infectados, downloads realizados em sites não confiáveis ou então podem existir pontos de vulnerabilidades em certos pontos de acesso.

Posteriormente a invasão o ransomware procura arquivos ou documentos que pode haver roubo de dados e então é feito o roubo dos dados e a criptografia dos mesmos e então podem fazer o bloqueio do dispositivo que foi infectado (computadores, celulares, etc).

5.1.1 CASOS DE CIBERATAQUES COM RANSOMWARE

Por conta da pandemia, de acordo com a Bitdefender, da qual analisou os dados da Rede de Proteção Global (GPN), os ataques de ransomware cresceram em 485% no ano de 2020 em comparação a 2019, sendo que 64% ocorreram apenas nos dois primeiros trimestres de 2020. Sendo que o Brasil ficou em nono lugar dos países que mais sofreram ataques em 2020, com mais de 3,8 milhões de ataques.

De uma forma geral, todas empresas e organizações de todos os tamanhos podem ser alvos de ataques ransomware, em bora o foco esteja em grandes empresas ou órgãos governamentais.

O Superior Tribunal de Justiça e o Ministério da Economia Brasileira já foram alvos de ataques com ransomware. Em ambos os casos, os criminosos alegaram ter criptografado dados de suma importância para os órgãos. A condição para a devolução das informações roubadas foi o pagamento de um valor definido pelos atacantes. Segundo as notícias consultadas, nenhum dos dois ataques causou danos significativos. No entanto, o vazamento de dados de órgãos como os dois citados é o bastante para causar grandes prejuízos a sociedade. Tratando-se do sistema judiciário, o vazamento ou perda de informações em segredo de justiça influência em condenações, penas, investigações e etc. Já no setor econômico, o vazamento de informações referentes a ações na bolsa de valores, por exemplo, pode causar grandes valorizações – ou desvalorizações – prejudicando não apenas os membros do quadro societário das empresas, mas também todos os seus empregados.

No setor privado, o escritório de advocacia Grubman Shire Meiselas e Sacks – que presta serviços para diversas celebridades – e a empresa de telecomunicações francesa Oragen – quarta maior empresa do ramo na Europa – também se tornaram vítimas desse tipo de ataque. Nesses dois casos, dados sigilosos de clientes das empresas foram roubados.

Como os casos citados demonstram, os ataques ransomwares não são prejudiciais somente para as vítimas diretas, mas também para todos os que dependem ou usam seus serviços, constatando a urgência e importância de mecanismos de prevenção e planos de contingência.

5.2. MECANISMOS DE DEFESA CONTRA RANSOMWARE

> Os ataques do tipo ransomware, que são uma preocupação mundial visto que se apresenta em franco crescimento e cada vez mais, possuem um alto grau tecnológico e que afeta a segurança dos dados e as comunicações. (LEMA, FREITAS, 2021).

Visto posto, existem uma série de cuidados e prevenções que podem ser tomadas para evitar ataques do tipo ransomware. Além das prevenções propriamente ditas, também é preciso investigar vulnerabilidades dentro do sistema, da rede e da própria infraestrutura. São exemplo comuns de vulnerabilidades: dispositivos e/ou softwares obsoletos e desatualizados; um plano de backup não abrangente o bastante, ou mesmo inexistente; falta de projetos e estratégias de cibersegurança.

Já as formas de prevenções são mais pautadas em boas práticas dos usuários da rede, já que o lado humano de um sistema – pessoal ou empresarial - sempre é o mais alvejado pelos criminosos. Entre as prevenções, pode-se citar: não fazer a divulgação de informações pessoais; não clicar em links ou abrir de procedência duvidosa; não utilizar pendrives desconhecidos; manter os programas e sistemas operacionais sempre atualizados; apenas realizar downloads de fontes confiáveis; preferencialmente não conectar-se a redes de Wi-Fi públicas, porém caso seja necessária a utilização de Wi-Fi públicos, é recomendável utilizar serviços de Rede Privada Virtual (VPN).

Também é necessário existir um plano de retirada de ransomwares do computador, pois se mesmo com toda a proteção e prevenção necessária tomada, acontecer alguma invasão, uma ação da deve ser realizada a fim de mitigar – e dependendo do caso até mesmo reverter completamente – os dados do ataque.

5.3. CIBERATAQUES COM RANSOMWARE EKANS

O ransomware Ekans - ou Snake - apareceu pela primeira vez em dezembro de 2019, escrito na linguagem de programação GO, uma linguagem comumente usada no desenvolvimento de malwares, pois é uma linguagem de fácil compilação para diversos sistemas operacionais, aumentando assim a abrangência dos ataques.

De acordo com o relatório de violação de dados da Verizon em 2020, o ransomware Ekans esteve presente em apenas um terço dos ataques com malware em 2019, conquanto quando este ransomware é direcionado a indústrias, uma infecção pode ser disruptiva e causar danos críticos, coagindo, assim, a um pagamento de resgate para que a ordem se reestabeleça.

Portanto o ransomware Ekans é direcionado, especificamente, a ICS (Sistemas de Controle Industrial), pois é capaz de desligar processos cruciais da indústria e, posteriormente, prossegue criptografando os dados e deixando uma nota de resgate com uma mensagem dos atacantes.

5.3.1 CASOS CIBERATAQUES COM RANSOMWARE EKANS

No mês de junho do ano de 2020 a empresa automobilística Honda registrou um ataque de ransomware. O ransomware utilizado em questão foi o Ekans – também chamado de Snake, “cobra” no idioma inglês. Este ocorrido paralisou diversas fábricas.

A Honda, por motivos evidentes, não informou por que meio os invasores conseguiram realizar o ataque e nem os reais danos do incidente, porém, segundo a reportagem pesquisada, a empresa afirmou que “os atacantes não

tinha apresentado qualquer evidência de perda e informações pessoalmente identificáveis”.

5.4. SIMULAÇÕES DE ATAQUES

Após a instalação das máquinas virtuais, conforme pode-se ver no Anexo A, foram feitas pesquisas sobre a linguagem de programação GO utilizada para desenvolver o ransomware em questão. Após as pesquisas tentou-se desenvolver um ransomware que fosse análogo ao Ekans para utilizar em uma simulação de ataque, porém durante as simulações realizadas com o ransomware desenvolvido, foi verificado que eram necessários conhecimentos em outras áreas para que o ransomware fosse suficientemente semelhante ao ransomware Ekans para que para se obter uma análise assertiva.

Atendando-se a isso foram realizadas pesquisas onde identificou-se que o INCIBE-CERT, centro de referência de resposta a incidentes de segurança para cidadãos e entidades de direito privado, operado pelo Instituto Nacional de Cibersegurança da Espanha (INCIBE), coletou amostras do ransomware Ekans e realizou uma análise detalhada de como o mesmo opera.

5.5. FUNCIONAMENTO DO RANSOMWARE EKANS

Baseando-se na análise realizada pelo INCIBE-CERT, verificou-se que o Ekans possui um padrão de propagação e operações semelhantes na maior parte de seus alvos, exceto para alguns ataques direcionados onde são criadas variações personalizadas. Em suma as infecções são realizadas por meio de uma configuração insegura de um Protocolo de Desktop Remoto (RDP), que é um protocolo que permite a utilização de um computador remotamente. Apesar dessa forma de contaminação ser a mais comum pode-se observar também que utilizam a infecção de pacotes de atualização legitimas e outros meios usuais, como spam contendo arquivos maliciosos.

O ransomware Ekans não possui rotinas de replicação, ou seja, para não ser perceptível o ransomware não se espalha pela rede de forma automática, o mesmo utiliza de scripts que são executados ao acessar o computador ou até

mesmo através de agendamentos de tarefas. O Ekans utiliza as funcionalidades de administração fornecidas pelo Windows para comprometer as infraestruturas através do Active Directory (AD), que é um banco de dados e um conjunto de serviços que conectam os usuários aos recursos de rede de que precisam para realizar seu trabalho, contendo assim informações do ambiente, usuários e computadores, além de conter informações sobre as permissões de acesso de cada usuário, além do mais o ransomware também utiliza outros serviços de gerenciamento típicos dos sistemas operacionais da Microsoft com o intuito de atingir o maior número de computadores possíveis.

Posteriormente a invasão o ransomware realiza uma verificação da existência de um mutex - objeto de programa que impede o acesso simultâneo a um recurso compartilhado - no computador, com a intenção de verificar se o mesmo foi infectado, caso ele já exista o Ekans encerra a sua execução e exibe uma mensagem em tela informando que os arquivos contidos no computador já foram criptografados, caso o mutex ainda não exista ele prossegue com a execução do código e captura o mutex com o nome “Global/EKANS”.

Subsequentemente o ransomware analisa se existe algum processo e serviço que corresponde à lista no código, caso exista o mesmo é interrompido através de uma função TerminateProcess(). Esses processos estão relacionados a sistemas SCADA (Sistema de Supervisão e Aquisição de Dados), ICS, máquinas virtuais, sistemas de administração de rede, entre outros.

Na próxima etapa o Ekans desabilita o serviço de cópia de sombra do Windows e exclui os backups para que não seja possível recuperar os dados criptografados. Após isso o mesmo busca parar todos os processos e serviços que são associados aos arquivos alvos de criptografia, para que não sejam mais bloqueados e a criptografia possa ocorrer sem falhas, os arquivos criptografados são localizados por sua extensão, com o intuito de não criptografar arquivos do sistema operacional para que o computador não seja desabilitado completamente e ainda seja possível mostrar a mensagem em tela para o usuário.

Para criptografar o mesmo gera uma chave AES-256 - chamado de padrão de criptografia avançada é uma especificação para a criptografia de dados eletrônicos estabelecida pelo instituto nacional de padrões e tecnologia

dos E.U.A - de 32 bytes utilizando como inicialização um vetor de 16 bytes, utilizando-se de uma função através de uma API (Interface de Programação de Aplicação) denominada CryptGenRandom, que geram os dados de criptografia de forma aleatória. A chave exclusiva é criptografada a partir da chave pública RSA-2048 – chamado de Rivest-Shamir-Adleman é um dos primeiros sistemas de criptografia de chave pública e é amplamente utilizado para transmissão segura de dados - está incorporada no próprio binário, e para incluir a chave criptografada, o vetor de inicialização e o nome do arquivo no final do arquivo criptografado o Ekans utiliza da codificação GOB da linguagem de programação GO.

Após os arquivos serem criptografados os mesmos são marcados com a string de texto “EKANS”, adicionando 5 caracteres aleatórios ao final do nome, portanto o ransomware trabalha da seguinte forma: primeiro seleciona os arquivos, posteriormente os criptografa e finalmente os renomeia, para que o usuário não perceba os sinais e aborte a operação antes que a mesma seja concluída.

A nota de resgate das informações e arquivos é gerado no arquivo de texto Decrypt-Your-Files.txt registrados em dois locais, um na unidade raiz do Windows e outro na área de trabalho do computador. As notas, escritas em inglês, contém detalhes do método utilizado para criptografia dos arquivos e e-mails para contatar os criminosos. O endereço de e-mail é usado pelo invasor para instruir as vítimas sobre o pagamento do resgate dos arquivos e informações.

5.6. MECANISMOS DE DEFESA PARA O RANSOMWARE EKANS

Portanto pode-se verificar que o Ekans, sendo um ransomware, possui mecanismos de defesa comuns, como por exemplo, manter a rede protegida com antivírus, treinamento de equipes sobre boas práticas da segurança da informação, manter os computadores e softwares atualizados, configurar permissões de acessos aos sistemas da empresa, realizar backups constantes em locais distintos, realizar boas práticas em geral e ter um plano de contingencia.

Entretanto, existe um mecanismo de defesa específico para este ransomware, que seria adicionar um mutex no computador, nominado de “Global/EKANS”, pois o ransomware verifica se já existe esse mutex no computador com o intuito de verificar se o mesmo já foi infectado ou não e caso ele já exista o ransomware interrompe a operação, outro mecanismo de defesa especifico para o Ekans.

6. DISCUSSÃO DOS RESULTADOS

O intuito do projeto foi verificar o funcionamento do ransomware Ekans e verificar quais seriam os melhores mecanismos de defesa para o mesmo, realizando simulações de ataques utilizando máquinas virtuais.

Contudo não foi possível realizar as simulações de ataques com satisfatoriedade, já que o ransomware é complexo, sendo necessário conhecimentos em muitas outras áreas de computação para reproduzi-lo, no entanto, foi possível verificar o seu funcionamento pois o INSIBE coletou amostras do ransomware e realizou uma análise detalhada do mesmo, onde foi visto que o Ekans foi especialmente desenvolvido para focar seus ataques na ICS e em toda a área relacionada à produção industrial, portanto este fato demonstra que quando existe uma invasão, há um comprometimento critico nos sistemas e nas infraestruturas de produção, afetando tanto cidadãos em geral quanto as empresas que a sofrem, gerando um grande impacto reputacional e econômico, diante disto, verificou-se a importância dos mecanismos de defesa e identificou-se quais mecanismos de defesa eram mais apropriados para o ransomware Ekans.

7. CONSIDERAÇÕES FINAIS

Assim podemos dizer que a pesquisa foi de grande valia, pois auxiliou a identificar os melhores meios de defesa para o ransomware Ekans e outros ransomwares em geral, cumprindo assim o seu objetivo previamente definido.

Além disso, a pesquisa contribuiu para entender novos conceitos em ciberataques e cibersegurança, ambos com importância atualmente, já que, não existe mais nenhum sistema que seja totalmente seguro.

Para trabalhos futuros sugere-se que haja um aprofundamento maior em conceitos da área de redes de computadores, criptografia de dados e a linguagem de programação GO, para que seja possível a replicação do ransomware Ekans com exatidão.

Conclui-se que o projeto foi de grande valia, gerando resultados que podem resultar no auxilio tomada de decisões de quais mecanismos de defesa serão utilizados e também a verificar o que será realizado caso aconteça uma invasão pelo ransomware Ekans e também contribuiu para o desenvolvimento acadêmico, profissional e intelectual da autora, desenvolvendo novas habilidades e conhecimentos.

8. REFERÊNCIAS

A DISTRIBUIÇÃO DE TESTE MAIS AVANÇADA. Disponível em: < https://www.kali.org/>. Acesso em: 25 de mar. de 2021.

ATAQUES DE RANSOMWARE BATE RECORDE E CRESCEM 485% EM 2020. Ciso Advisor, 2021. Disponível em: < https://www.cisoadvisor.com.br/ataques-de-ransomware-batem-recorde-e-crescem-485-em-2020/#:~:text=Os%20ataques%20de%20ransomware%20aumentaram,na%20pandemia%20de%20covid%20%2D19. >. Acesso em: 14 de dez. De 2021.

BASÍLIO, A. L. O que é um ciberataque?. CartaCapital, 2017. Disponível em: < https://www.cartacapital.com.br/carta-explica/o-que-e-um-ciberataque/>. Acesso em: 19 de mar. De 2021.

BRASIL É UM DOS PAÍSES QUE MAIS SOFRERAM ATAQUES DE RANSOMWARE EM 2020. Ciso Advisor, 2021. Disponível em: < https://www.cisoadvisor.com.br/brasil-e-um-dos-paises-que-mais-sofreram-ataques-de-ransomware-em-2020/ >. Acesso em: 14 de dez. De 2021.

CARDOSO, P. O que é um ransomware?. TechTudo, 2017. Disponível em: < https://www.techtudo.com.br/noticias/noticia/2016/06/o-que-e-ransomware.html>. Acesso em: 22 de mar. de 2021.

ESTATÍSTICAS DOS INCIDENTES REPORTADOS AO CERT.BR. CERT.br, 2020. Disponível em: < https://www.cert.br/stats/incidentes/>. Acesso em: 18 de mar. de 2021.

GIL. A. C.; Como Elaborar Projetos de Pesquisa. 5.ed. São Paulo: Atlas, 2010.

INCIDENTES REPORTADOS AO CERT.BR. CERT.br, 2020. Disponível em: < https://cert.br/stats/incidentes/2020-jan-jun/tipos-ataque.html >. Acesso em: 19 de mar. de 2021.

INFORMAÇÃO. In: DICIONÁRIO Aurélio da Língua Portuguesa. 8. ed. Curitiba: Editora Positivo, 2010. v. 2, p. 426.

KASPERSKY ANALIZA RANSOMWARE QUE PARALISOU INDUSTRIAS DO MUNDO. Inforchannel, 2020. Disponível em: < https://inforchannel.com.br/2020/06/24/kaspersky-analisa-ransomware-que-paralisou-industrias-no-mundo/ >. Acesso em: 14 de dez. De 2021.

LEMA, FREITAS. Ataques Ransomware. Seminario de Tecnologia e Educãção, 2021. Disponível em: < http://raam.alcidesmaya.edu.br/index.php/SGTE/article/view/326>. Acesso em: 22 de ma. de 2022.

MUTUAL EXCLUSION (MUTEX). Techopedia. Disponível em: < https://www.techopedia.com/definition/25629/mutual-exclusion-mutex >. Acesso em: 15 de jul. de 2022.

O QUE É O ACTIVE DIRECTORY? CONHEÇA O AD E COMO ELE FUNCIONA. Quest. Disponível em: < https://www.quest.com/br-pt/solutions/active-directory/what-is-active-directory.aspx >. Acesso em: 20 de jul. De 2022.

O QUE É UM RANSOMWERE?. Kaspersky. Disponível em: < https://www.kaspersky.com.br/resource-center/definitions/what-is-ransomware >. Acesso em: 22 de mar. de 2021.

ORACLE VM VIRTUALBOX. Oracle. Disponível em: < https://www.oracle.com/br/virtualization/virtualbox/>. Acesso em: 25 de mar. De 2021.

PRINCIPAIS ATAQUES DE RANSOMWARE. Kaspersky. Disponível em: < https://www.kaspersky.com.br/resource-center/threats/top-ransomware-2020 >. Acesso em: 14 de dez. de 2021

RANSOMWARE EKANS: CARACTERÍSTICAS Y FUNCIONAMIENTO. INCIBE. Disponível em: < https://www.incibe-cert.es/blog/ransomware-ekans-caracteristicas-y-funcionamiento >. Acesso em: 6 de jul. de 2022.

SEGURANÇA. In: DICIONÁRIO Aurélio da Língua Portuguesa. 8. ed. Curitiba: Editora Positivo, 2010. v. 2, p. 689.

SPAFFORD, G.; Diretor de Operações de Computador, Auditoria e Tecnologia da Segurança, Purdue University/France.

ZEFERINO, D. O que são ciberataques, como acontecem e como prevenir?. Certifiquei, 2020. Disponível em: < https://www.certifiquei.com.br/ciberataques/ >. Acesso em: 19 de mar. De 2021.

9. APENDICE

APENDICE A – Instalação das Máquinas Virtuais

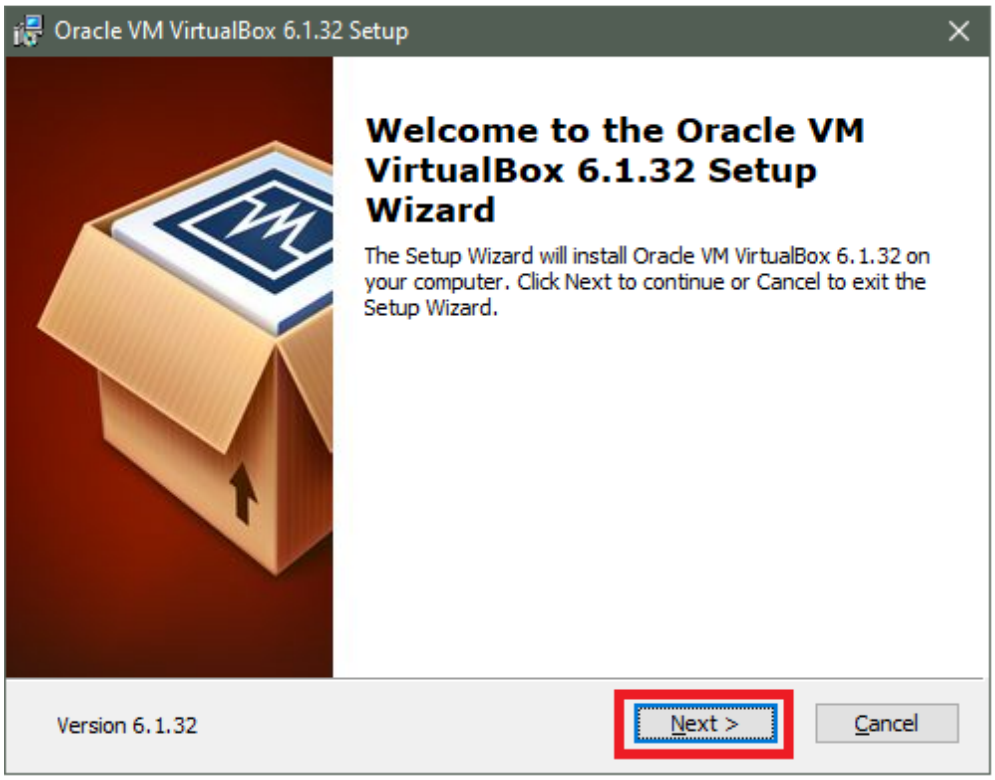
Para instalação das máquinas virtuais, foi feito primeiramente o download no site da VirtualBox, clicando na opção Windows Hosts, conforme mostrado na Figura 1.

Figura 1 – Download VirtualBox

Fonte: Elaborada pela Autora.

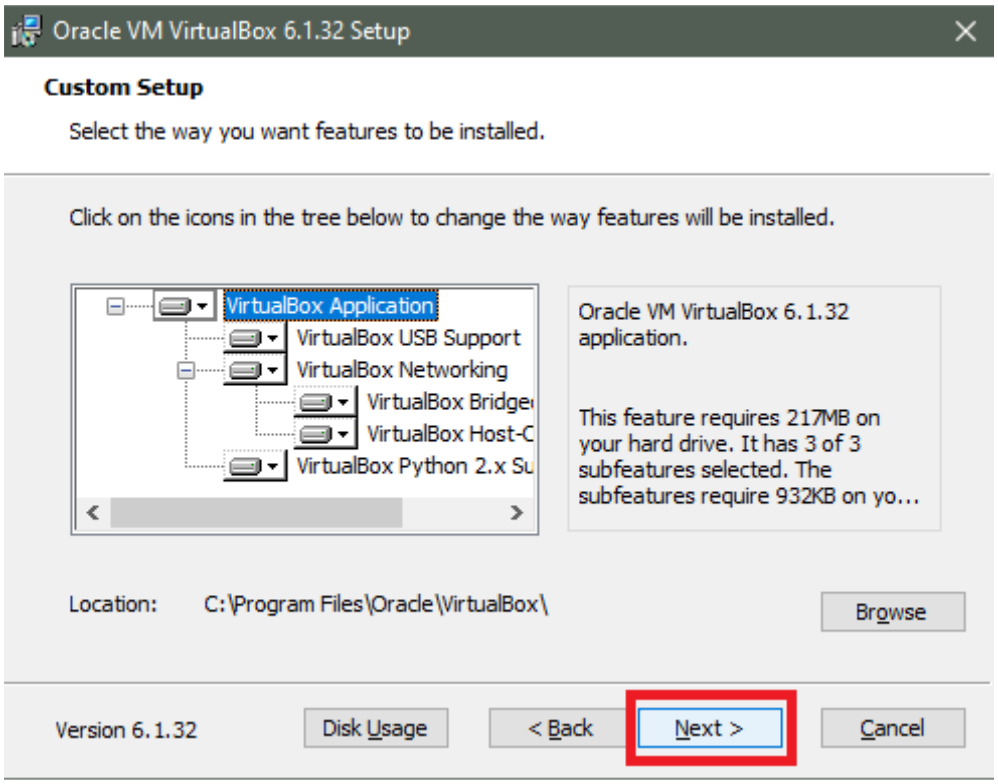
Então foi realizada instalação da VirtualBox seguindo os passos a seguir como pode ser visto da Figuras 2 até a Figura 8.

Figura 2 – Instalação VirtualBox



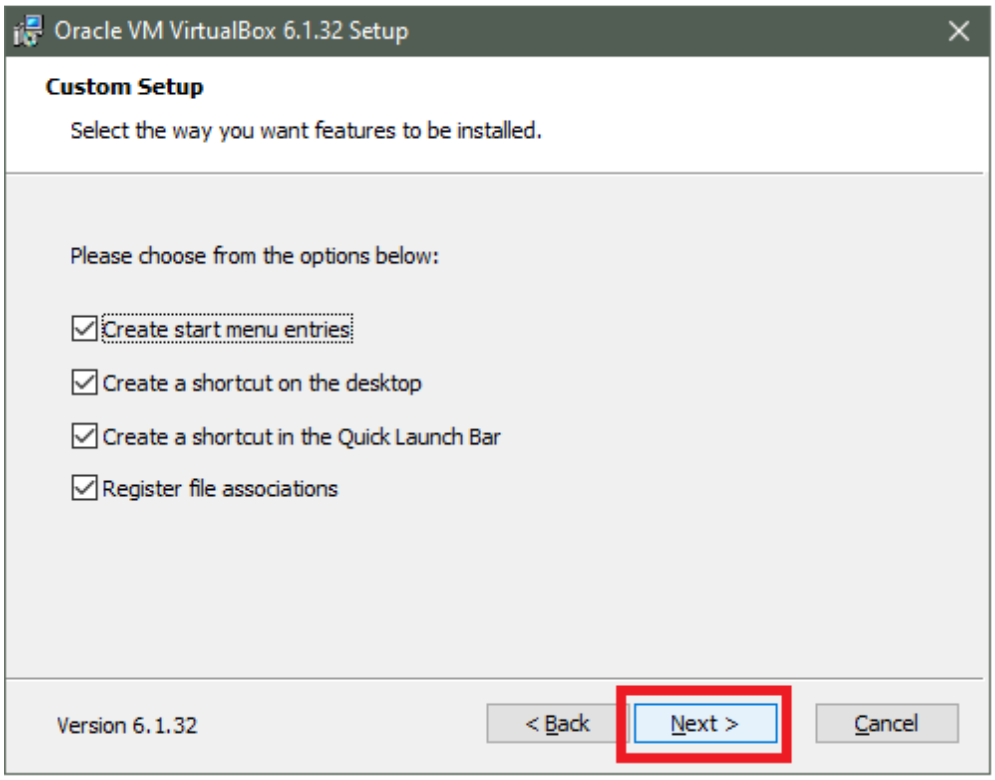
Fonte: Elaborada pela Autora.

Figura 3 – Instalação VirtualBox



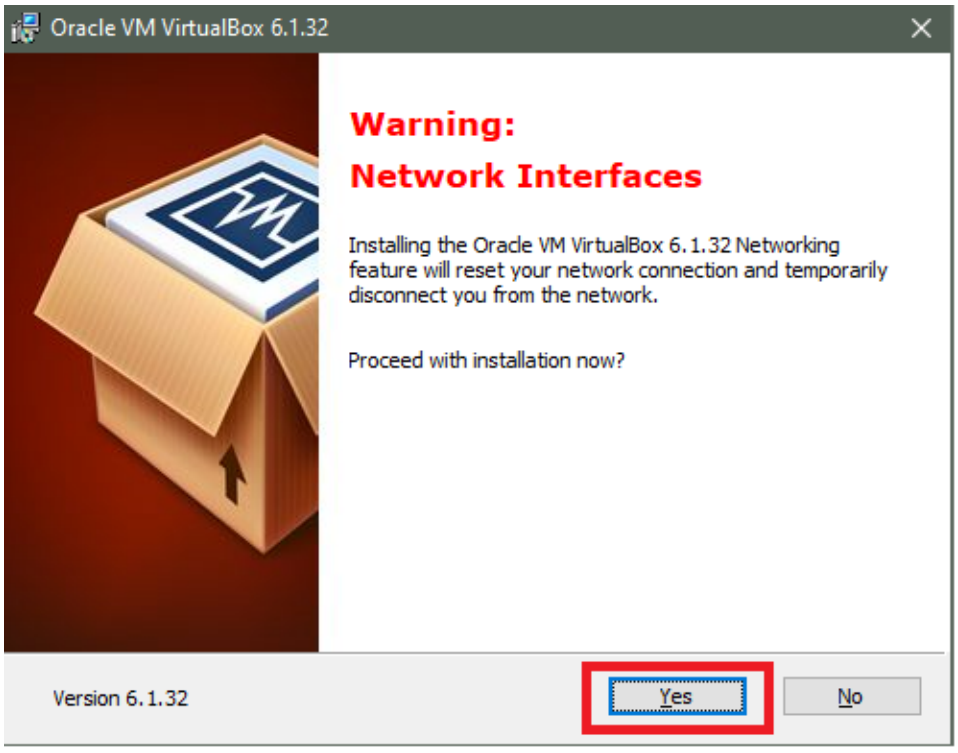
Fonte: Elaborada pela Autora.

Figura 4 – Instalação VirtualBox



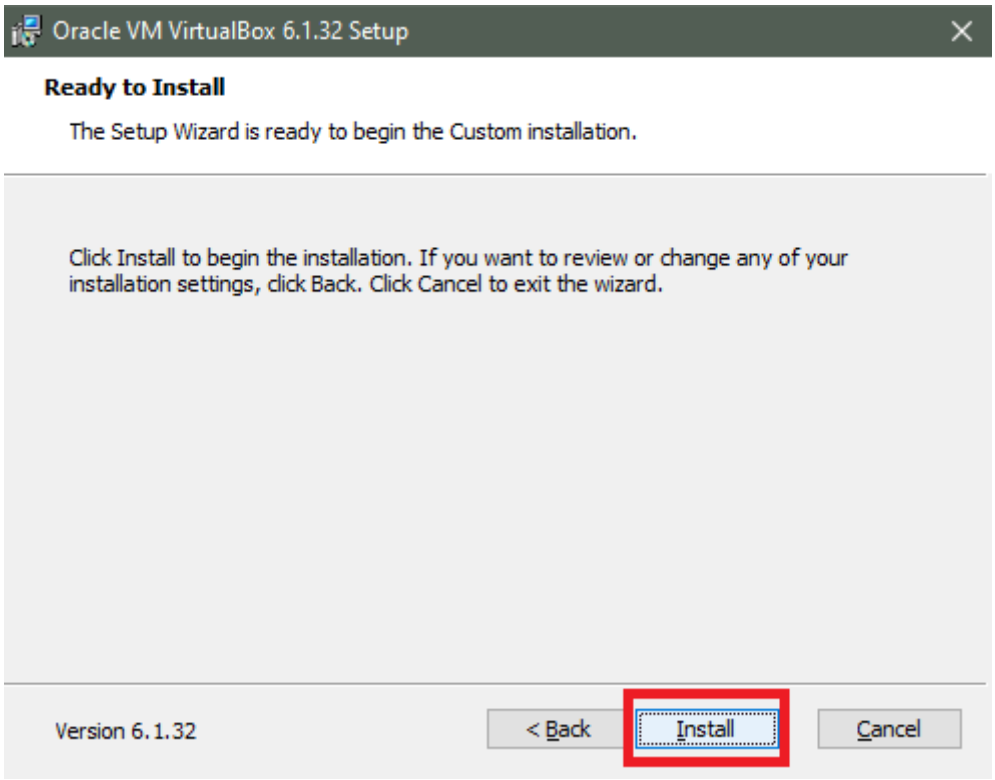
Fonte: Elaborada pela Autora.

Figura 5 – Instalação VirtualBox



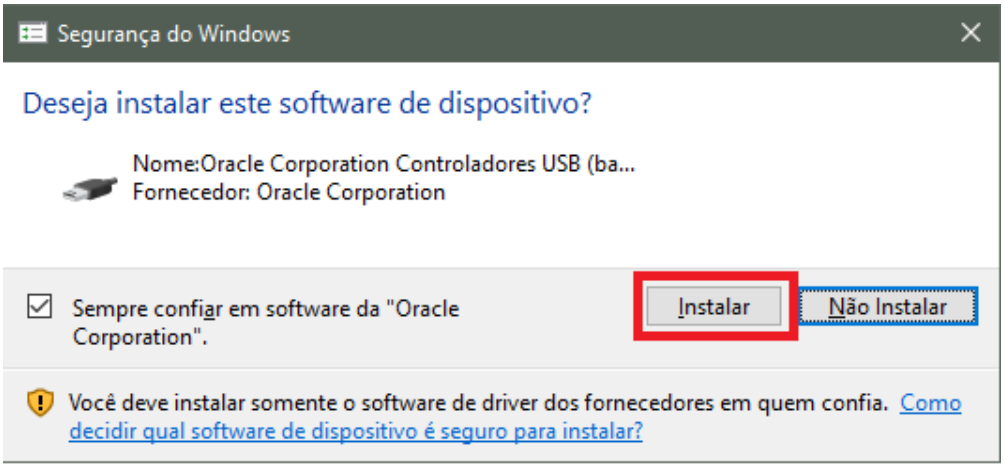
Fonte: Elaborada pela Autora.

Figura 6 – Instalação VirtualBox



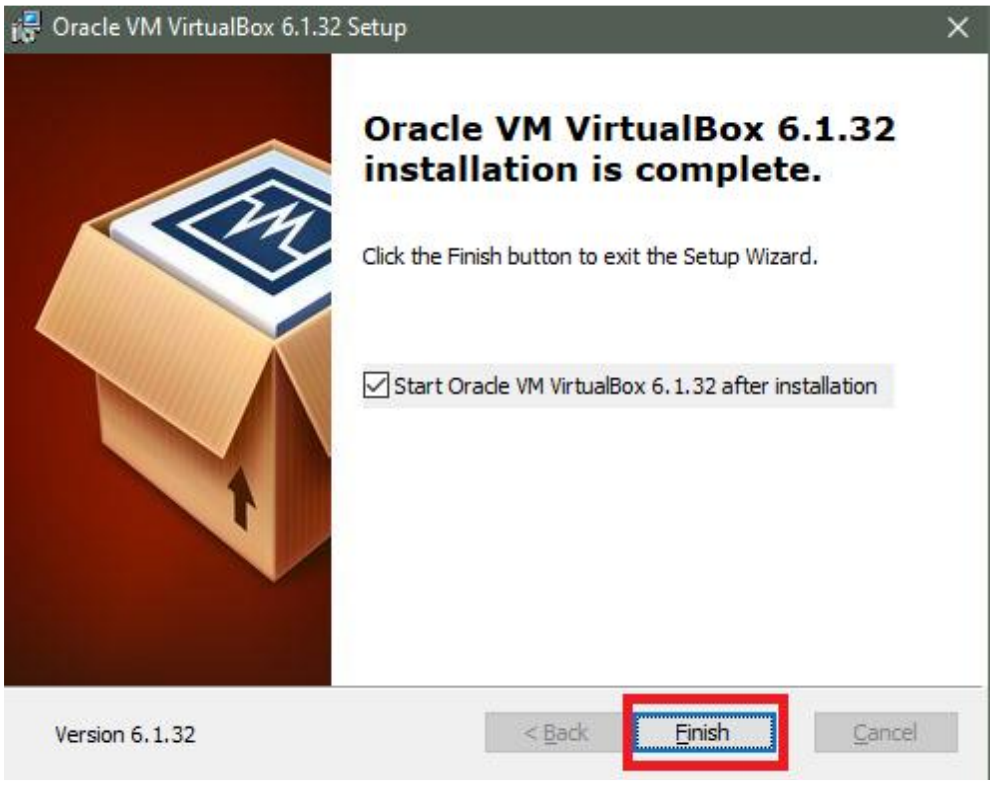
Fonte: Elaborada pela Autora.

Figura 7 – Instalação VirtualBox



Fonte: Elaborada pela Autora.

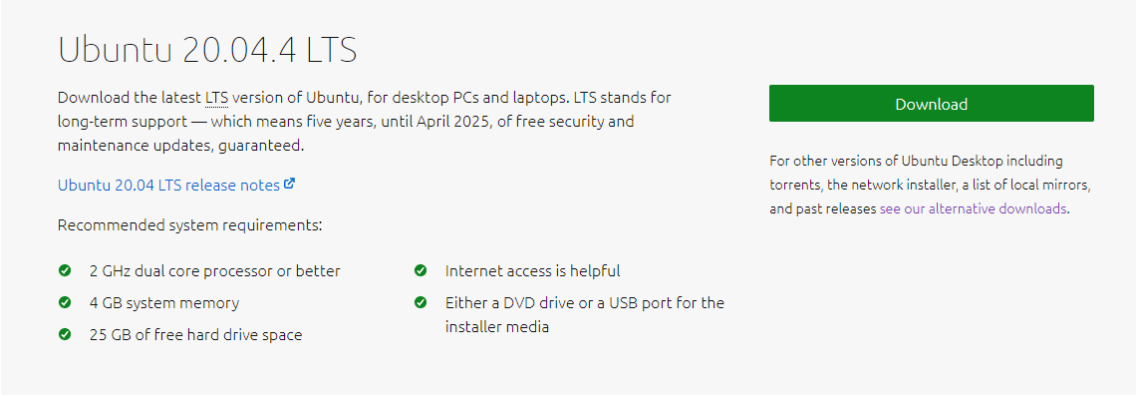
Figura 8 – Instalação VirtualBox



Fonte: Elaborada pela Autora.

Posteriormente foi realizado o download do sistema operacional Linux Ubuntu, no próprio site da Ubuntu, conforme mostrado na Figura 9.

Figura 9 – Download Sistema Operacional Linux



Fonte: Elaborada pela Autora.

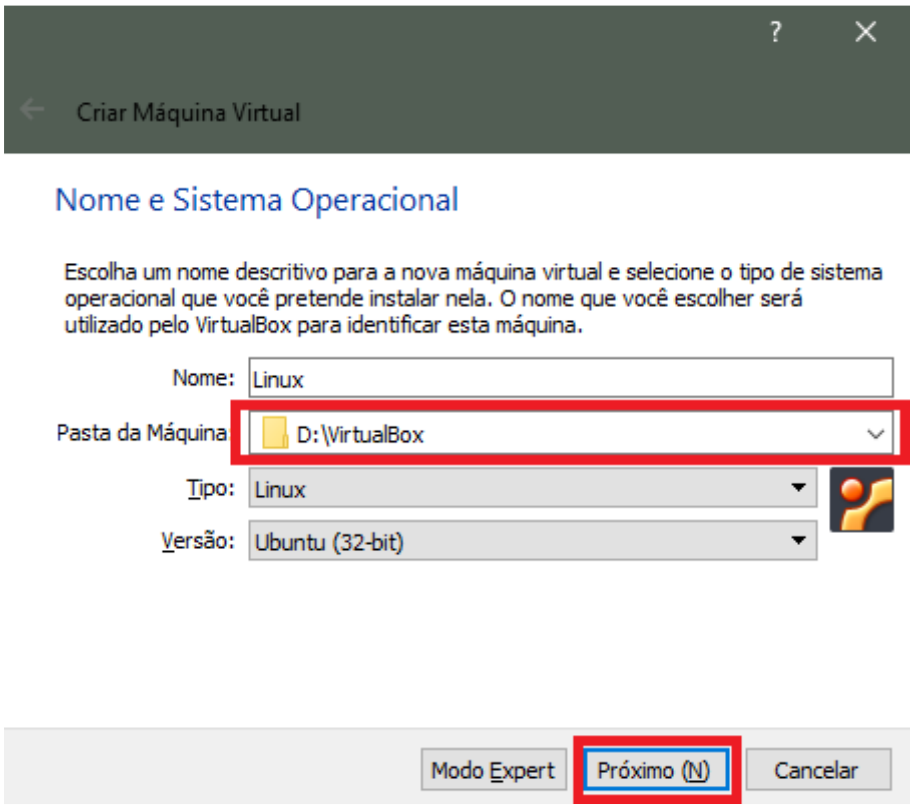
Primeiramente é necessário abrir a VM e clicar em novo, para criar uma máquina virtual, como é possível visualizar na Figura 10.

Figura 10 – Criação de uma VM

Fonte: Elaborada pela Autora.

Primeiro é preciso selecionar a pasta onde está o download do sistema operacional e clicar em próximo (Figura11).

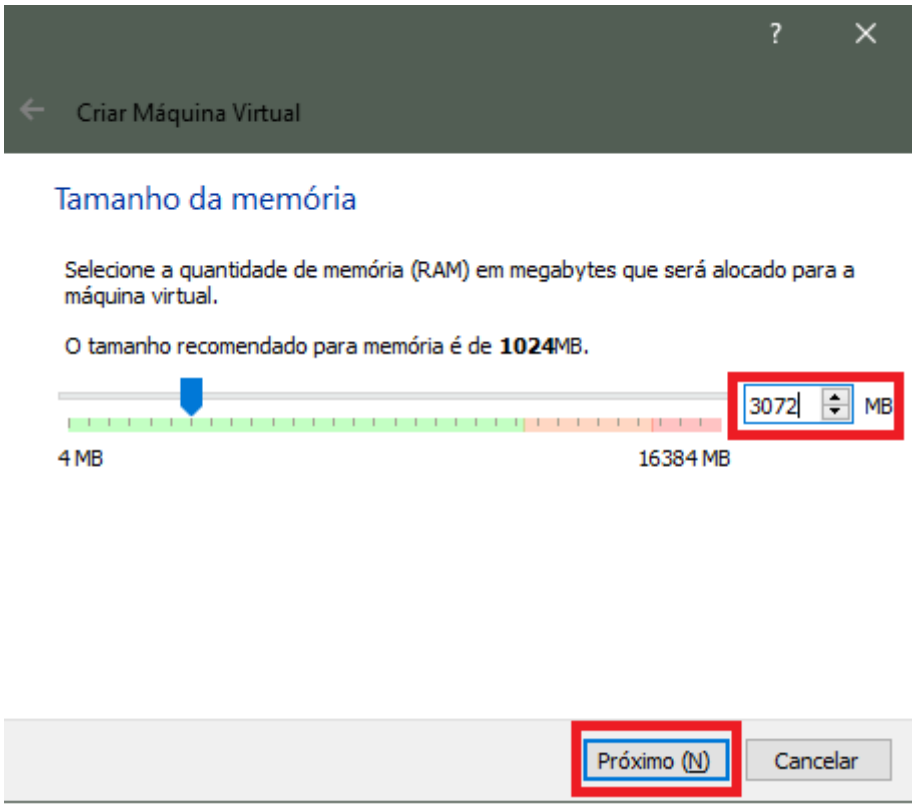
Figura 11 – Selecionando o Sistema Operacional Linux



Fonte: Elaborada pela Autora.

A máquina virtual exige uma quantidade de memória, da máquina física, que será utilizada por ela, portanto foi necessário selecionar essa quantidade conforme e clicar em próximo a Figura 12 a seguir.

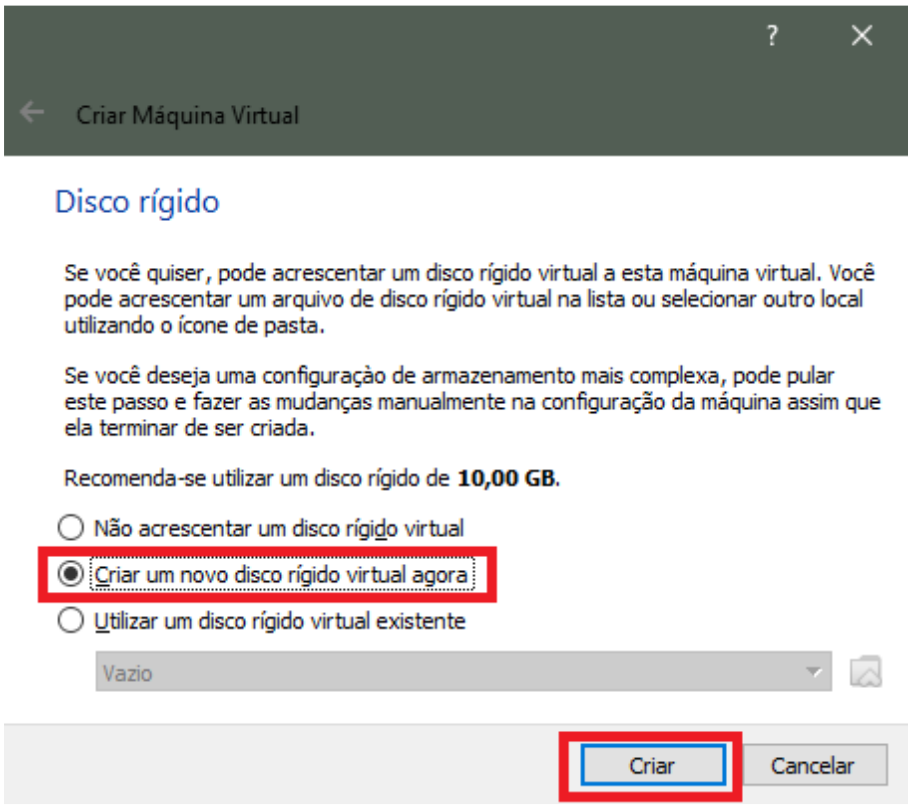
Figura 12 – Selecionando Quantidade de Memória



Fonte: Elaborada pela Autora.

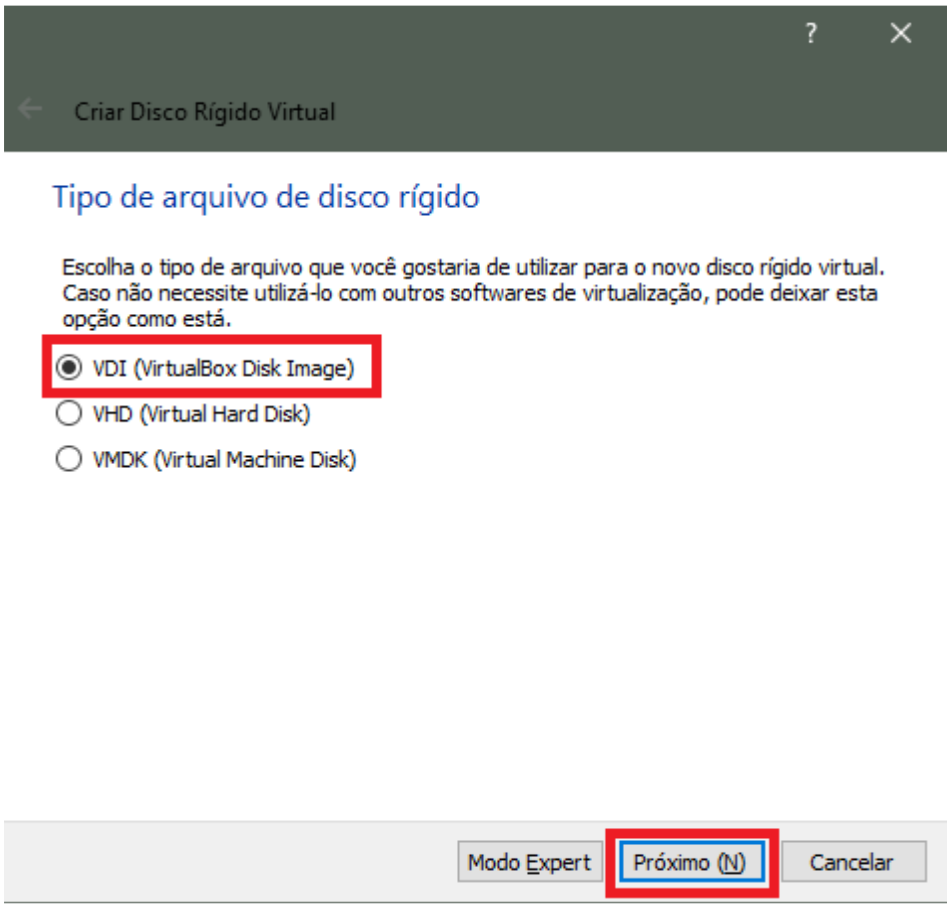
O mesmo processo é necessário para a criação do disco rígido, para isso podemos criar conforme os passos a seguir das Figuras 13 a 17.

Figura 13 – Criação do Disco Rígido



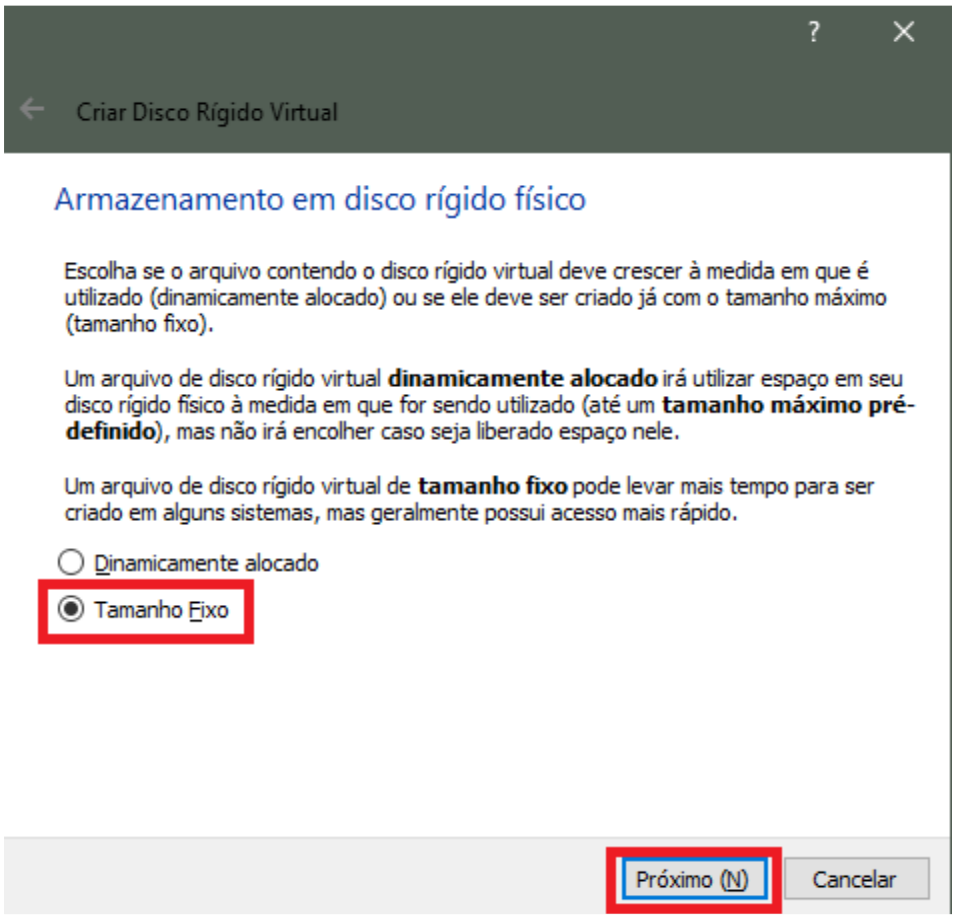
Fonte: Elaborada pela Autora.

Figura 14 – Criação do Disco Rígido



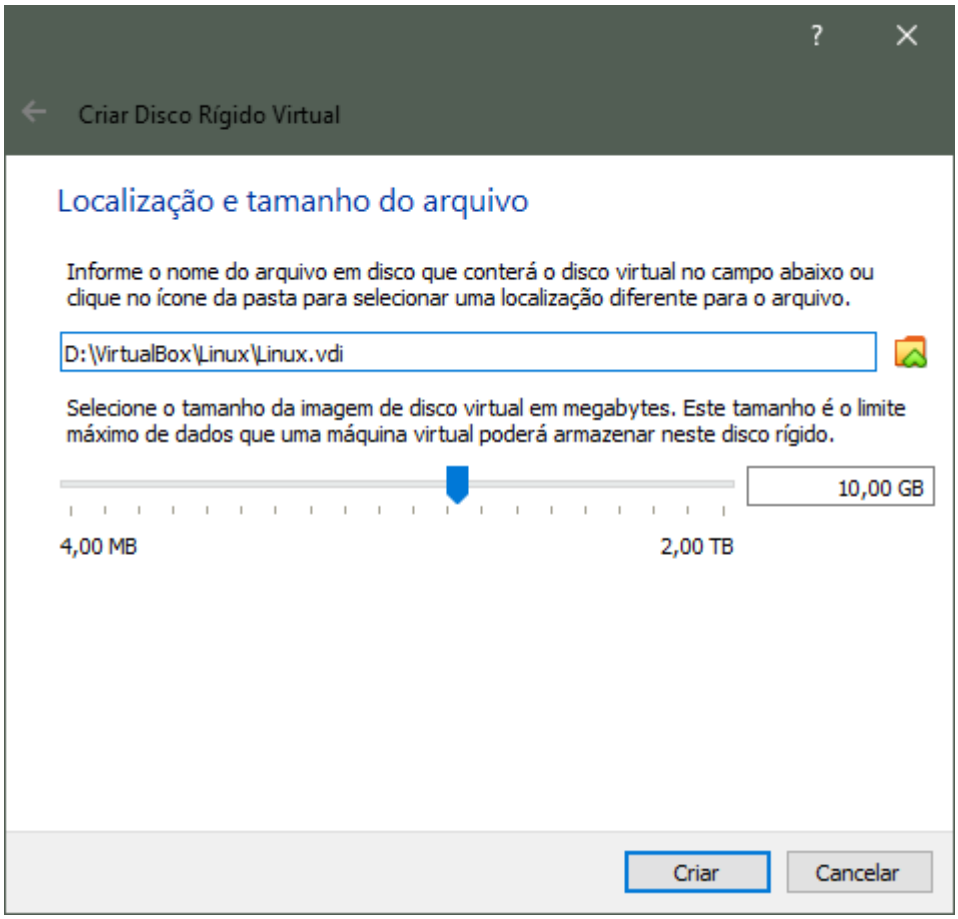
Fonte: Elaborada pela Autora.

Figura 15 – Criação do Disco Rígido



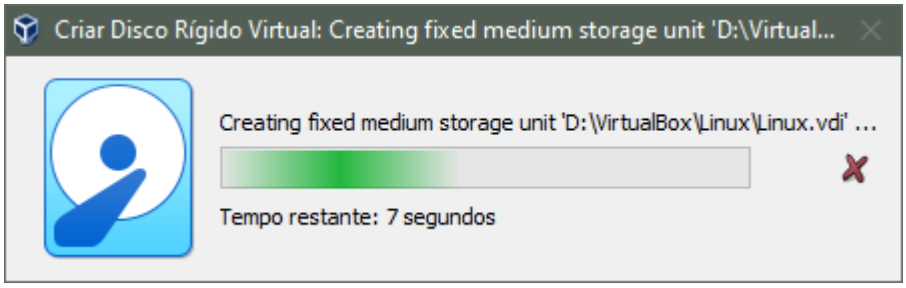
Fonte: Elaborada pela Autora.

Figura 16 – Criação do Disco Rígido



Fonte: Elaborada pela Autora.

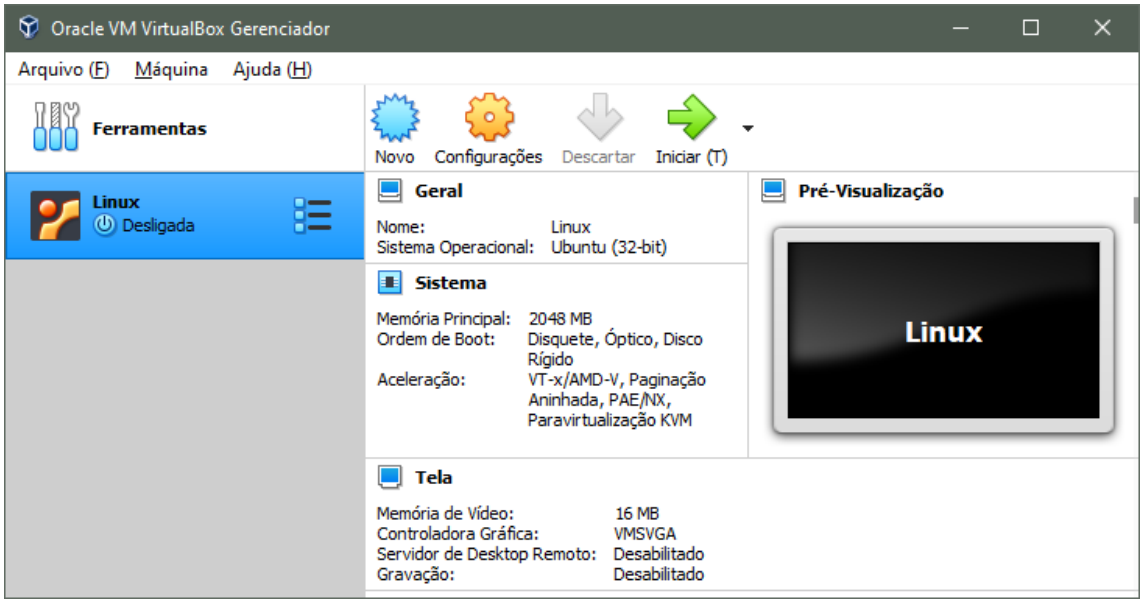
Figura 17 – Criação do Disco Rígido



Fonte: Elaborada pela Autora.

Posteriormente a isso pode-se ver a VM criada. (Figura 18).

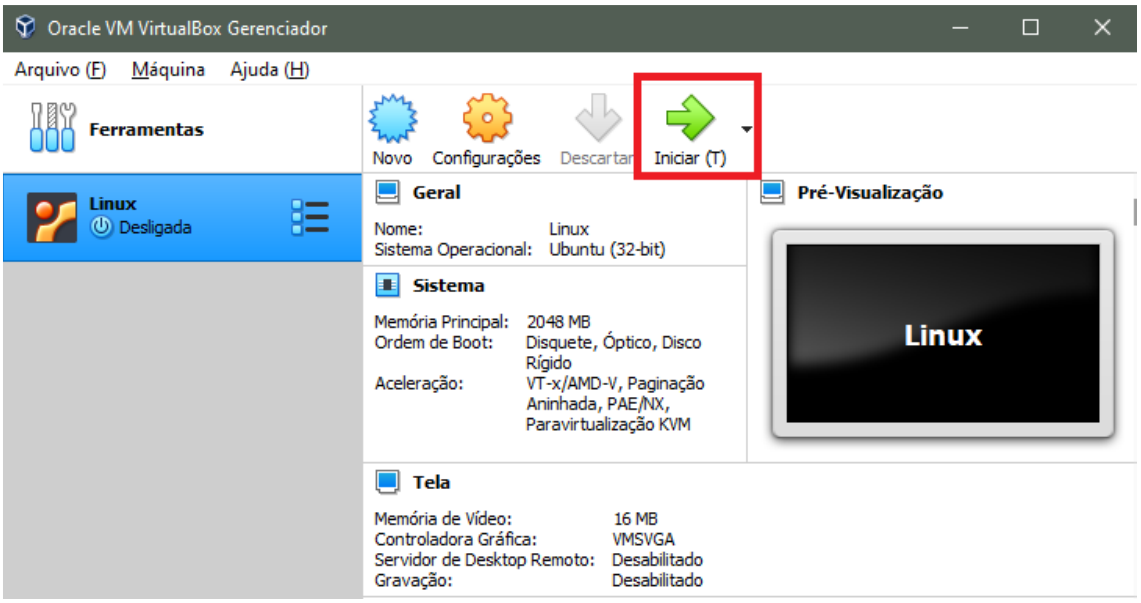
Figura 18 – VM criada



Fonte: Elaborada pela Autora.

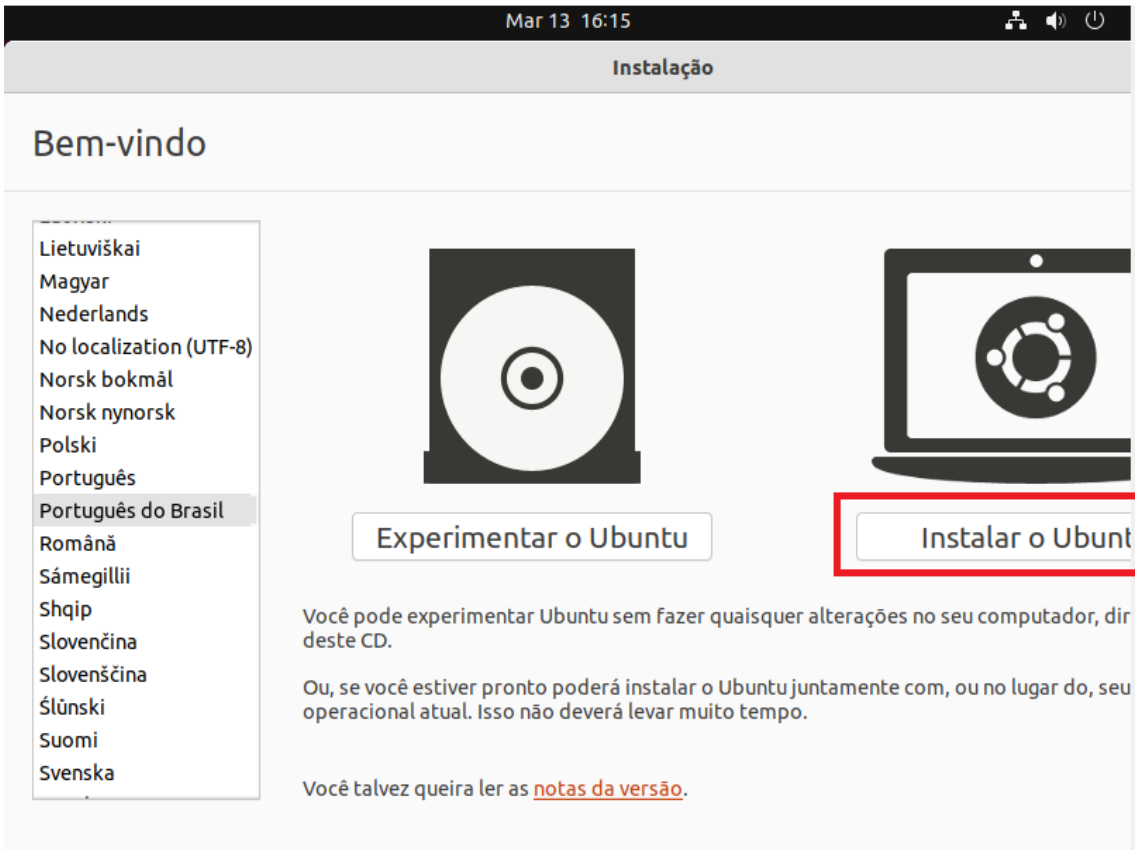
Subsequentemente foi realizada a instalação do sistema operacional e do usuário, como pode se visualizar nas Figuras 19 a 28.

Figura 19 – Instalação Sistema Operacional Linux



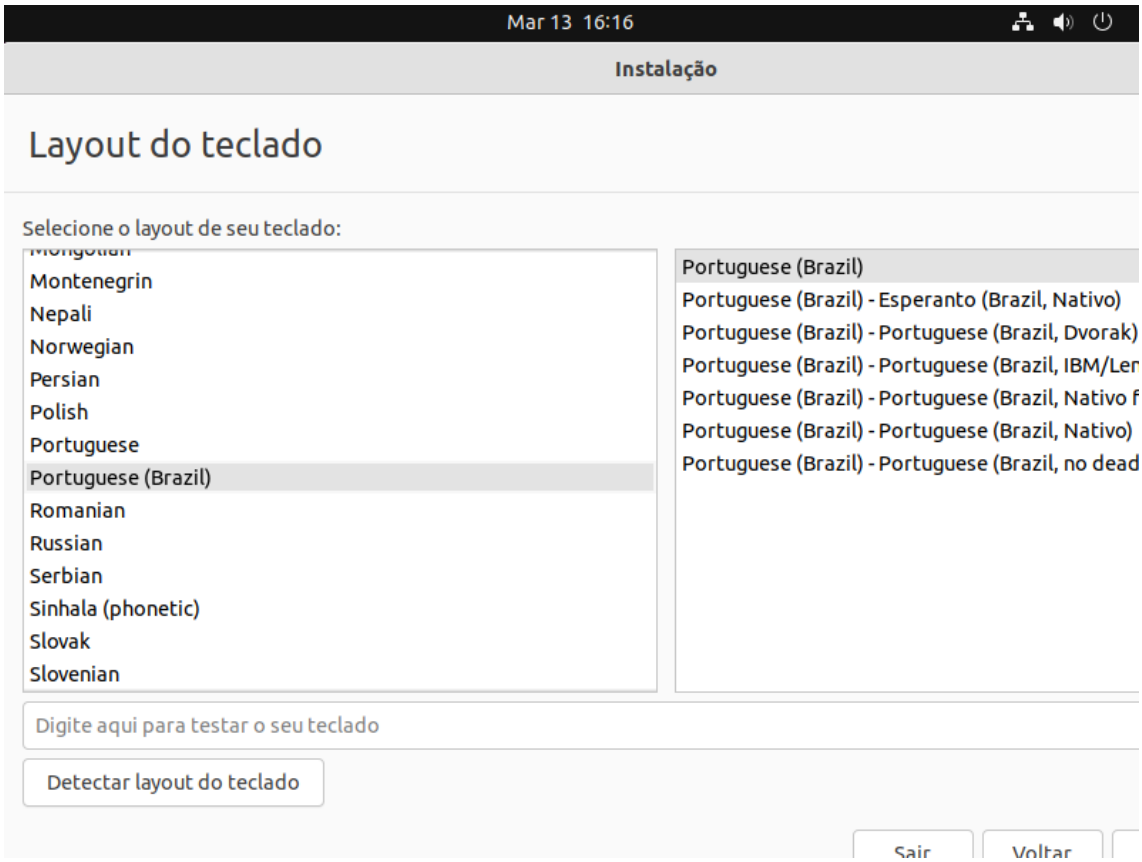
Fonte: Elaborada pela Autora.

Figura 20 – Instalação Sistema Operacional Linux



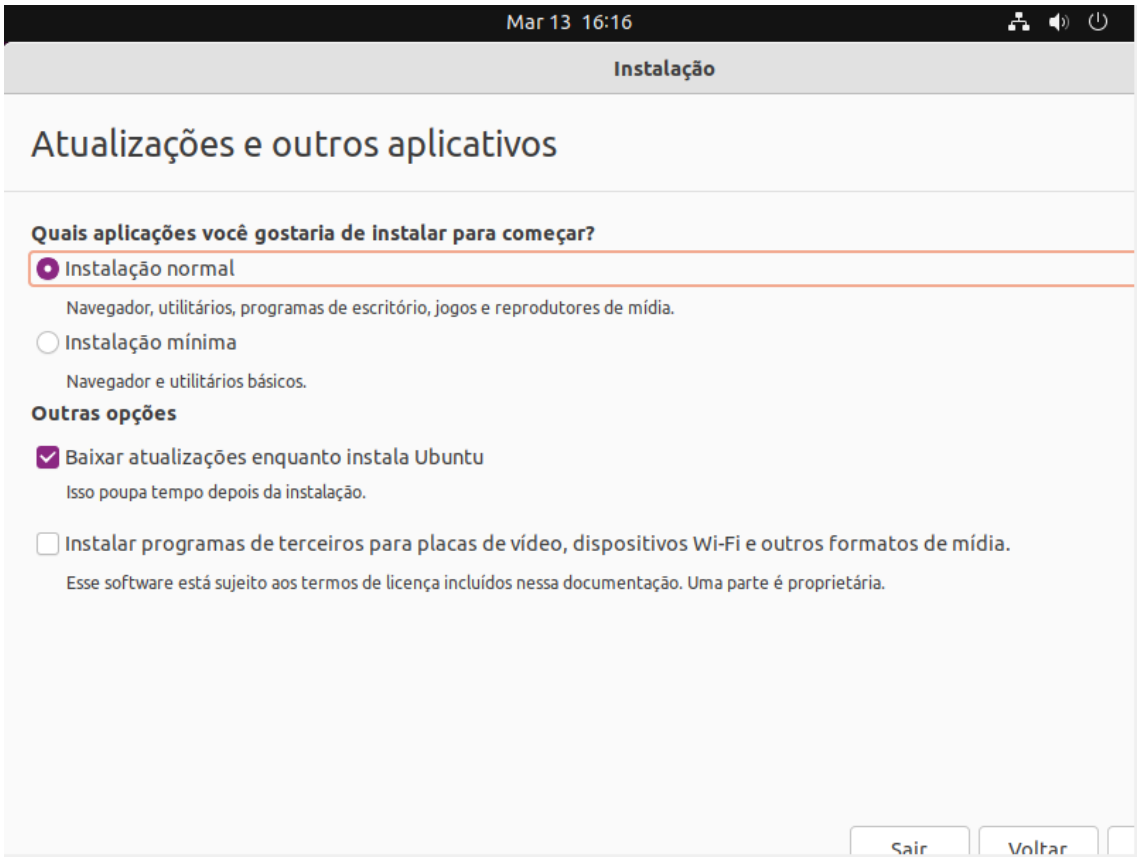
Fonte: Elaborada pela Autora.

Figura 21 – Instalação Sistema Operacional Linux



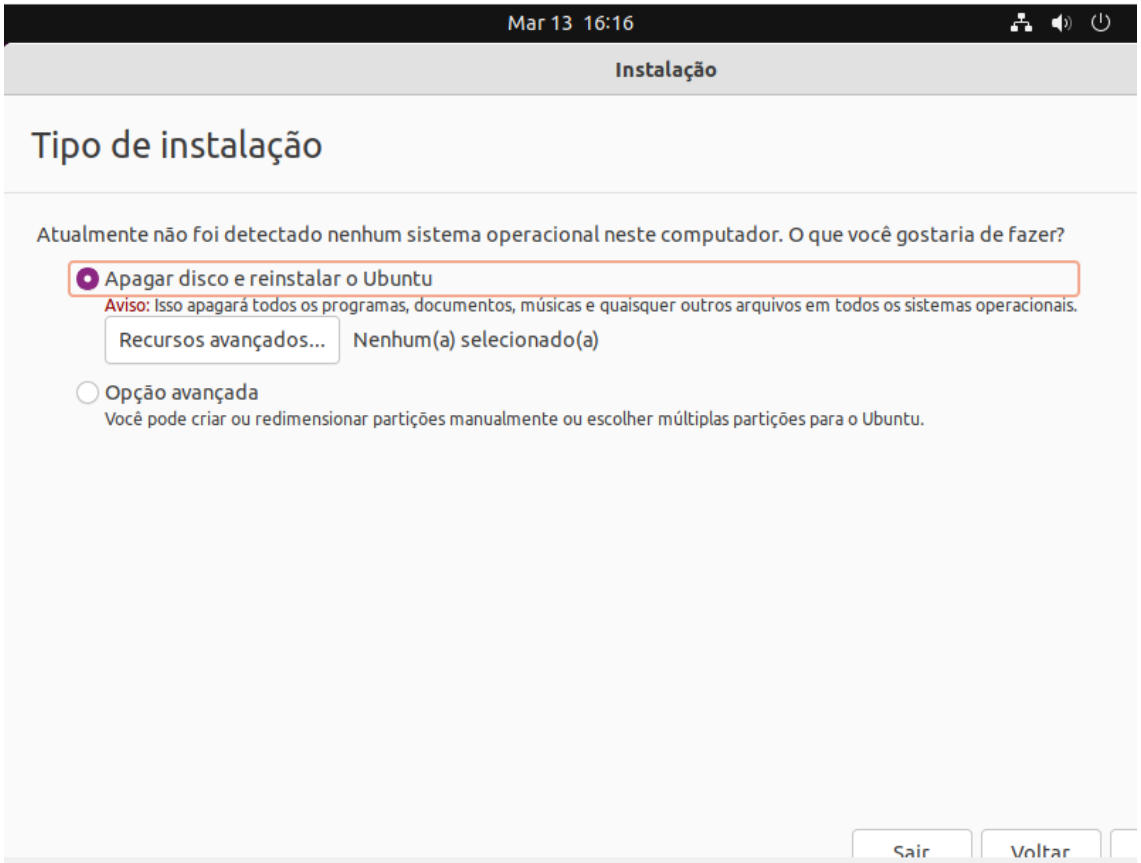
Fonte: Elaborada pela Autora.

Figura 22 – Instalação Sistema Operacional Linux



Fonte: Elaborada pela Autora.

Figura 23 – Instalação Sistema Operacional Linux

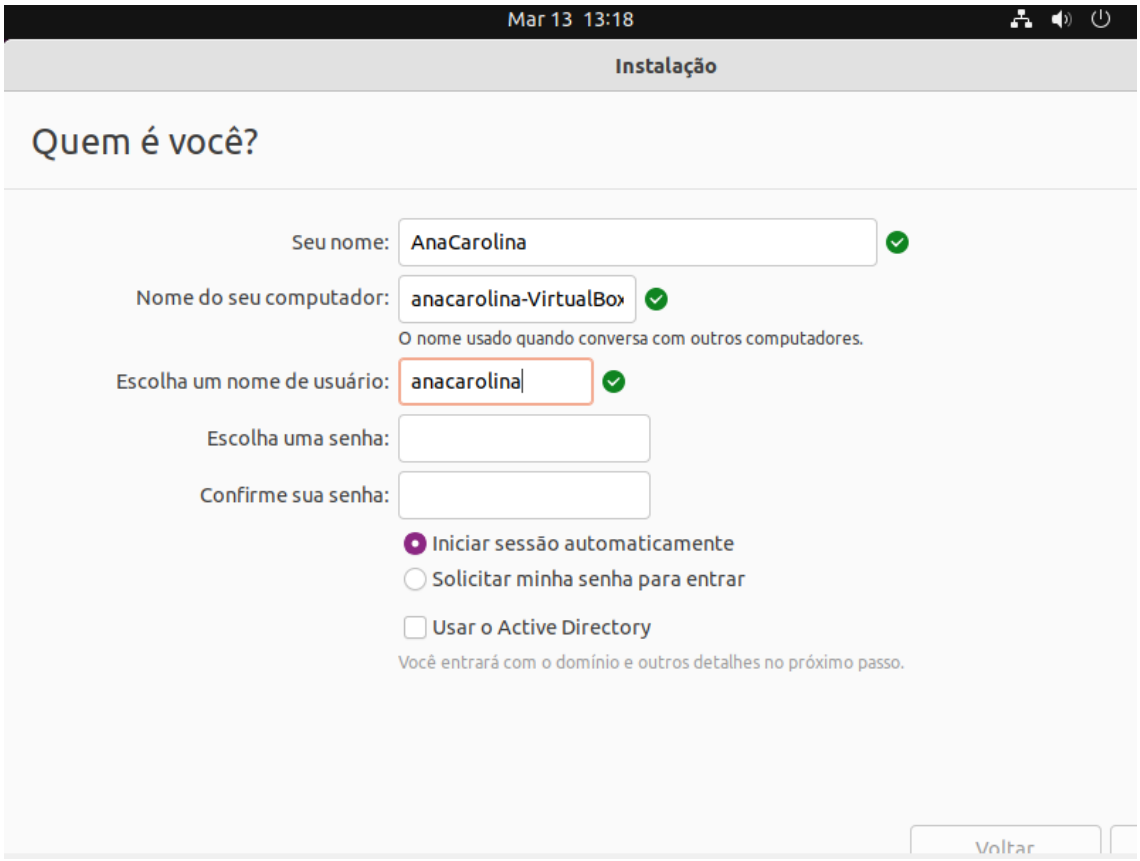


Fonte: Elaborada pela Autora.

Figura 24 – Instalação Sistema Operacional Linux

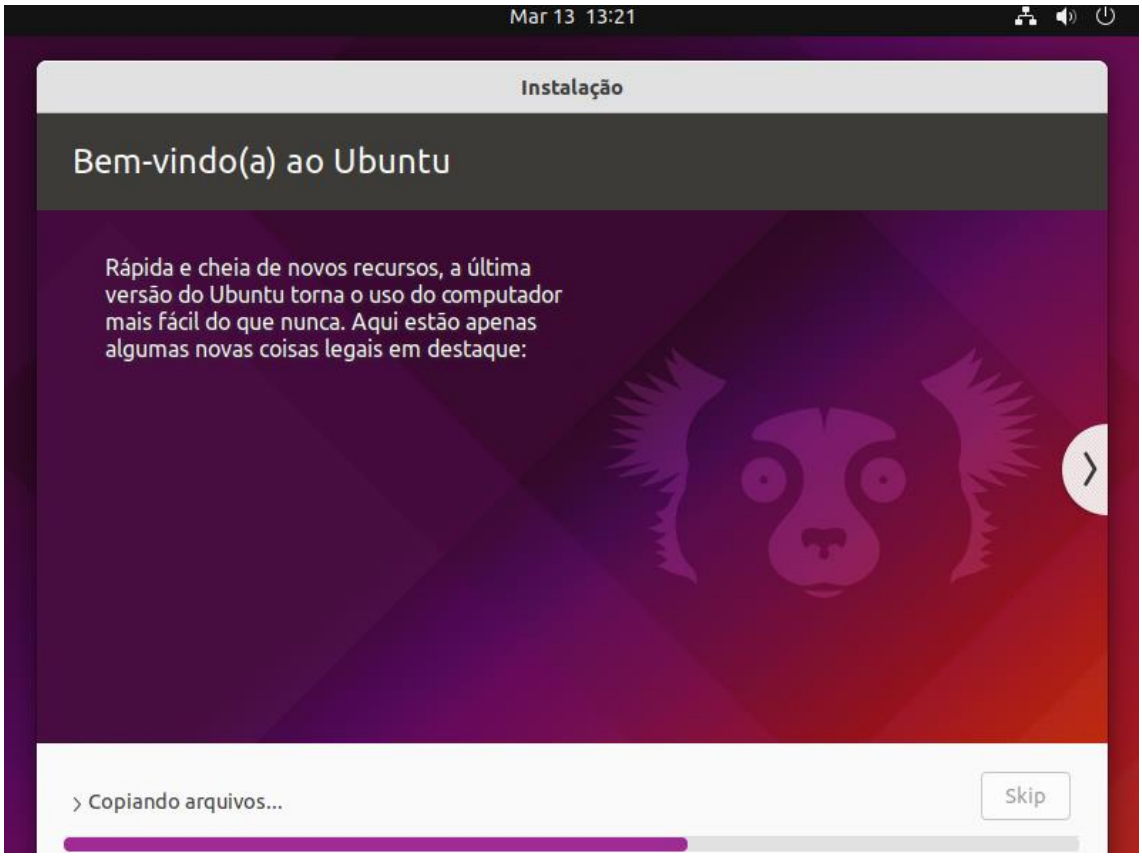
Fonte: Elaborada pela Autora.

Figura 25 – Instalação Sistema Operacional Linux



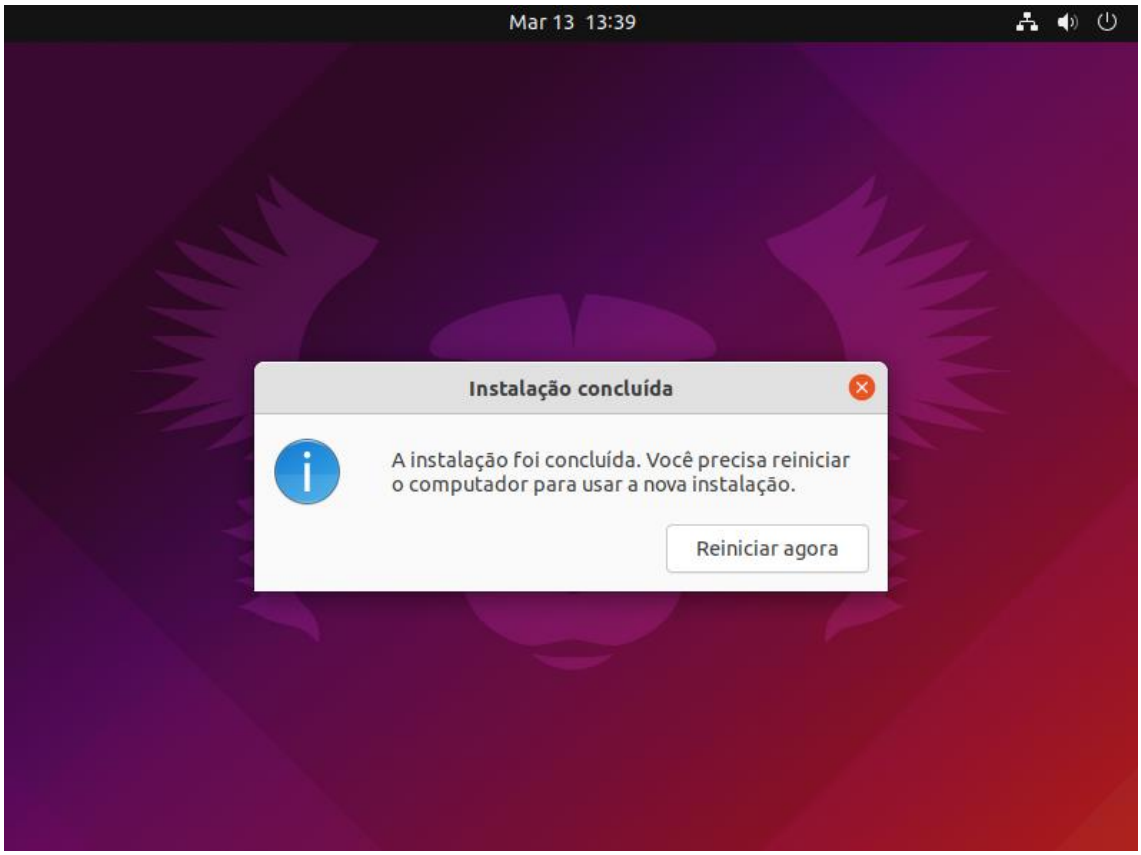
Fonte: Elaborada pela Autora.

Figura 26 – Instalação Sistema Operacional Linux



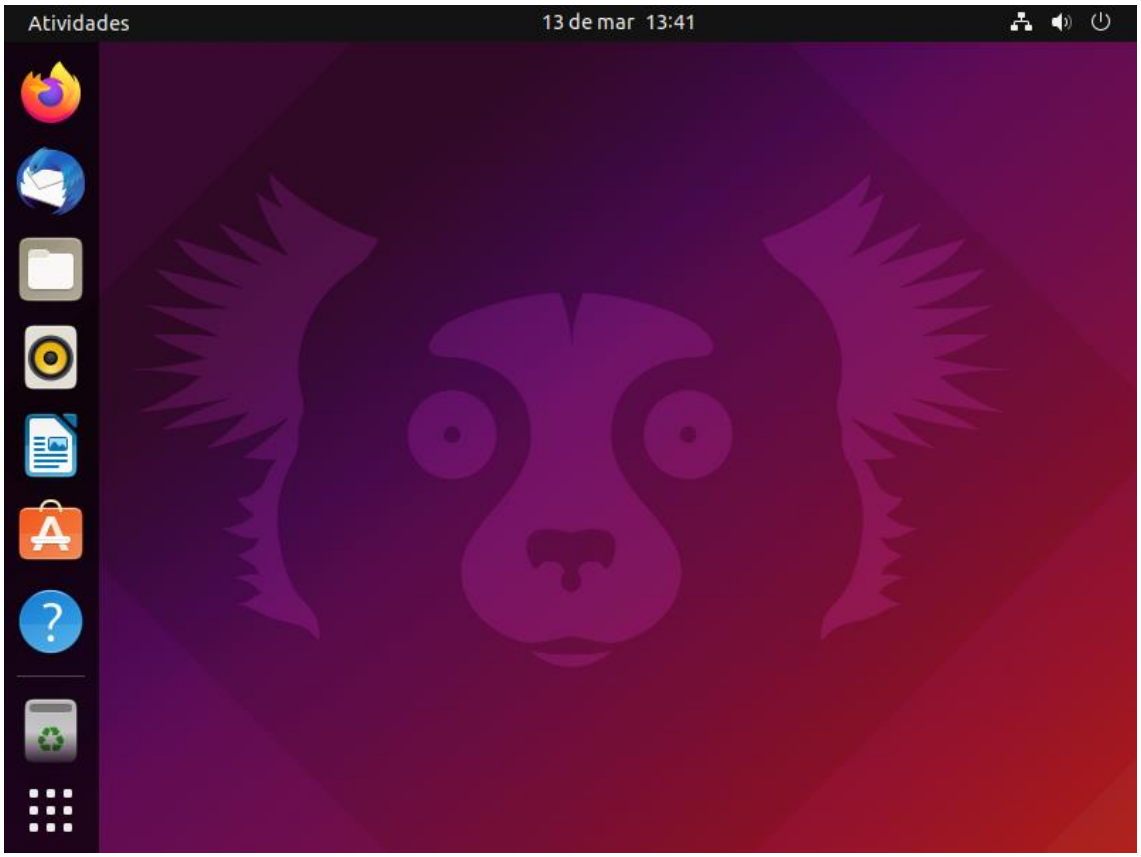
Fonte: Elaborada pela Autora.

Figura 27 – Instalação Sistema Operacional Linux



Fonte: Elaborada pela Autora.

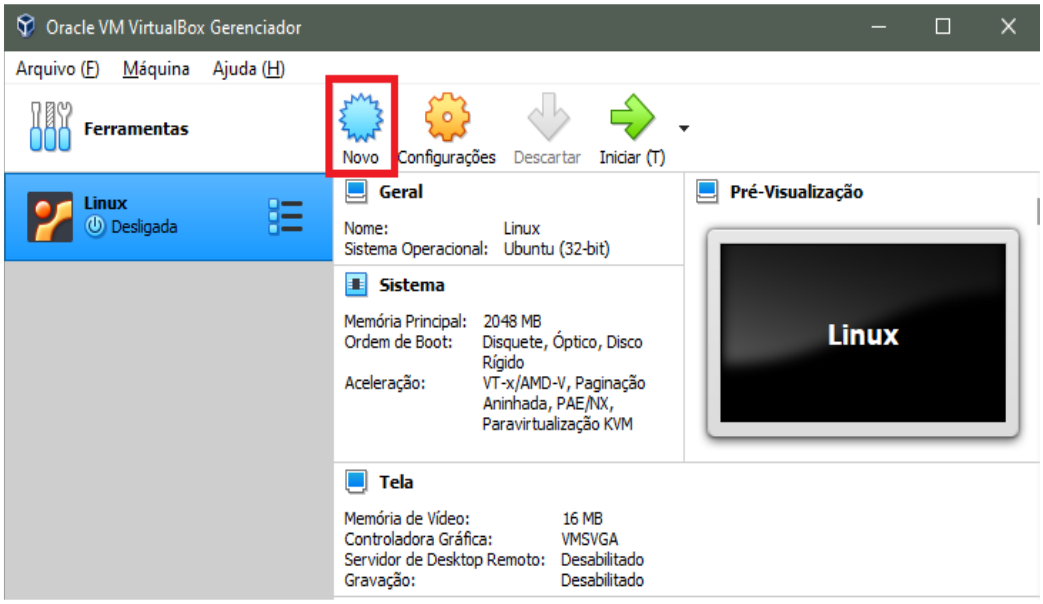
Figura 28 – Instalação Sistema Operacional Linux



Fonte: Elaborada pela Autora.

Para a criação da segunda VM foi necessário clicar em novo, para criar uma outra máquina virtual como é possível visualizar na Figura 29. E então seguir os mesmos passos seguidos anteriormente.

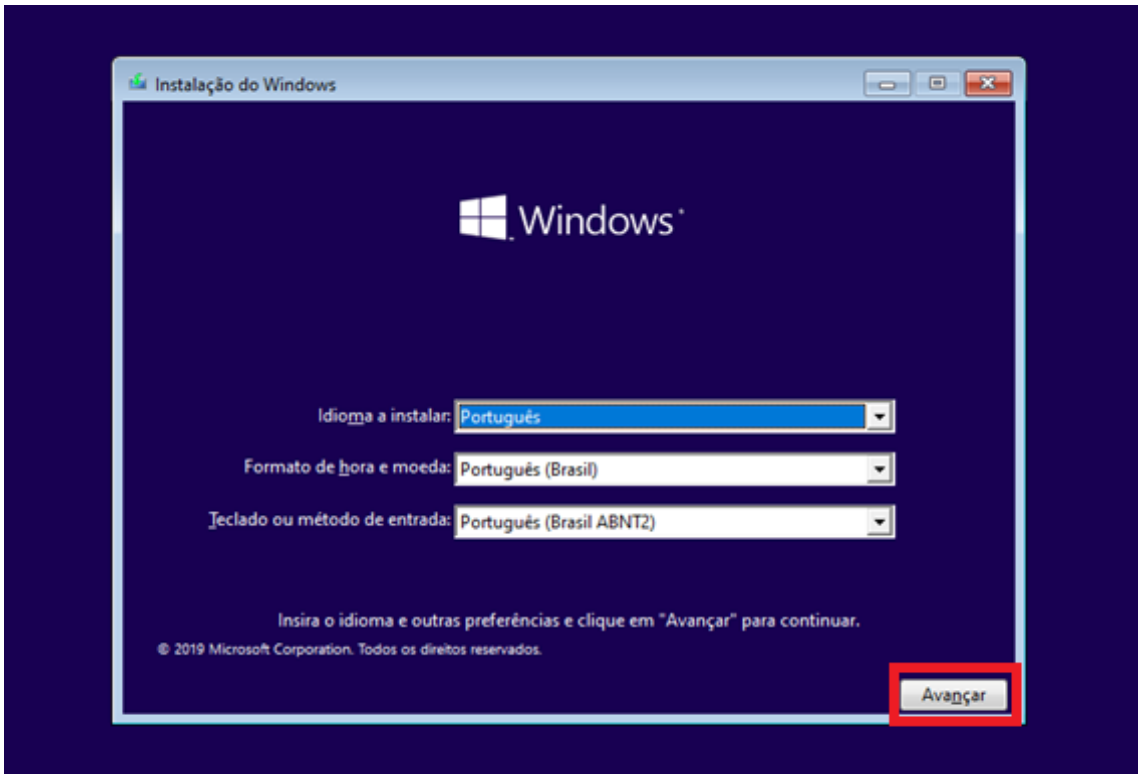
Figura 29 – Criação de Segunda VM



Fonte: Elaborada pela Autora.

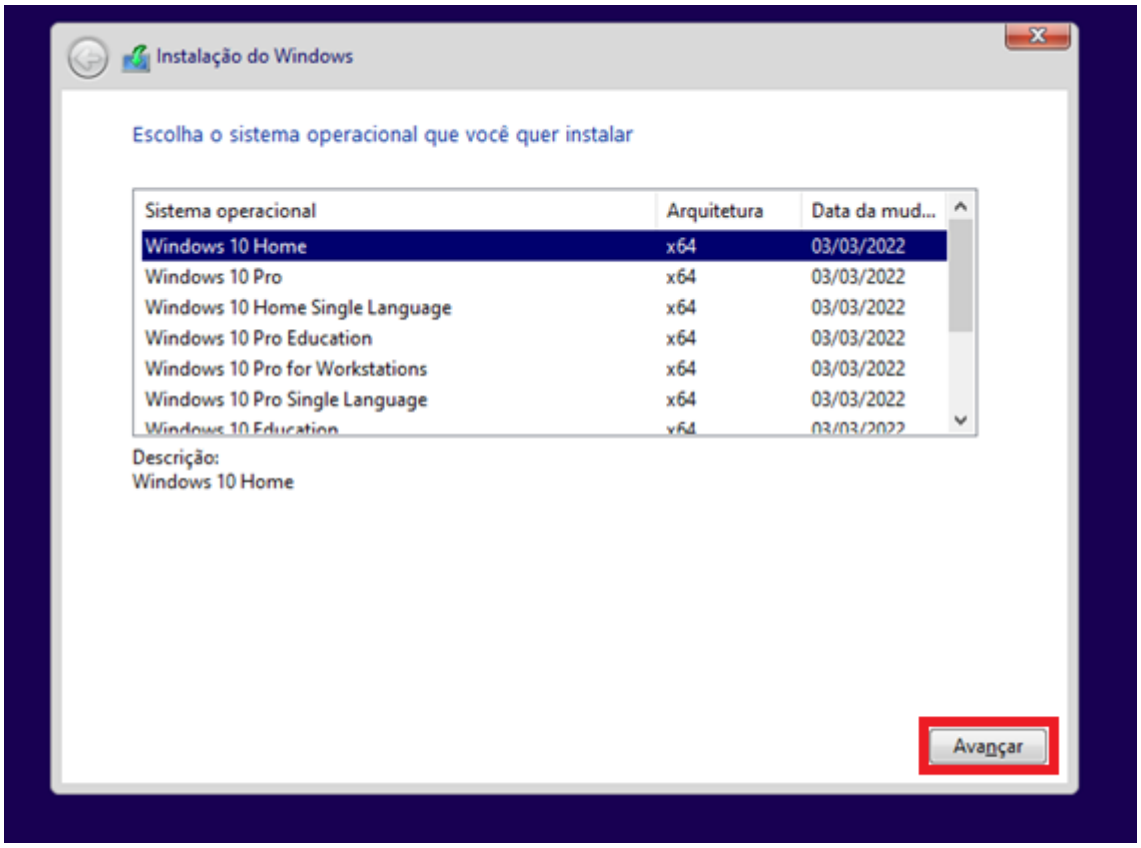
Então para a instalação do sistema operacional da segunda VM (Windows Home), clica-se em Iniciar e seguiremos os passos a seguir, conforme as Figuras 30 a 34.

Figura 30 – Instalação do Sistema Operacional Windows



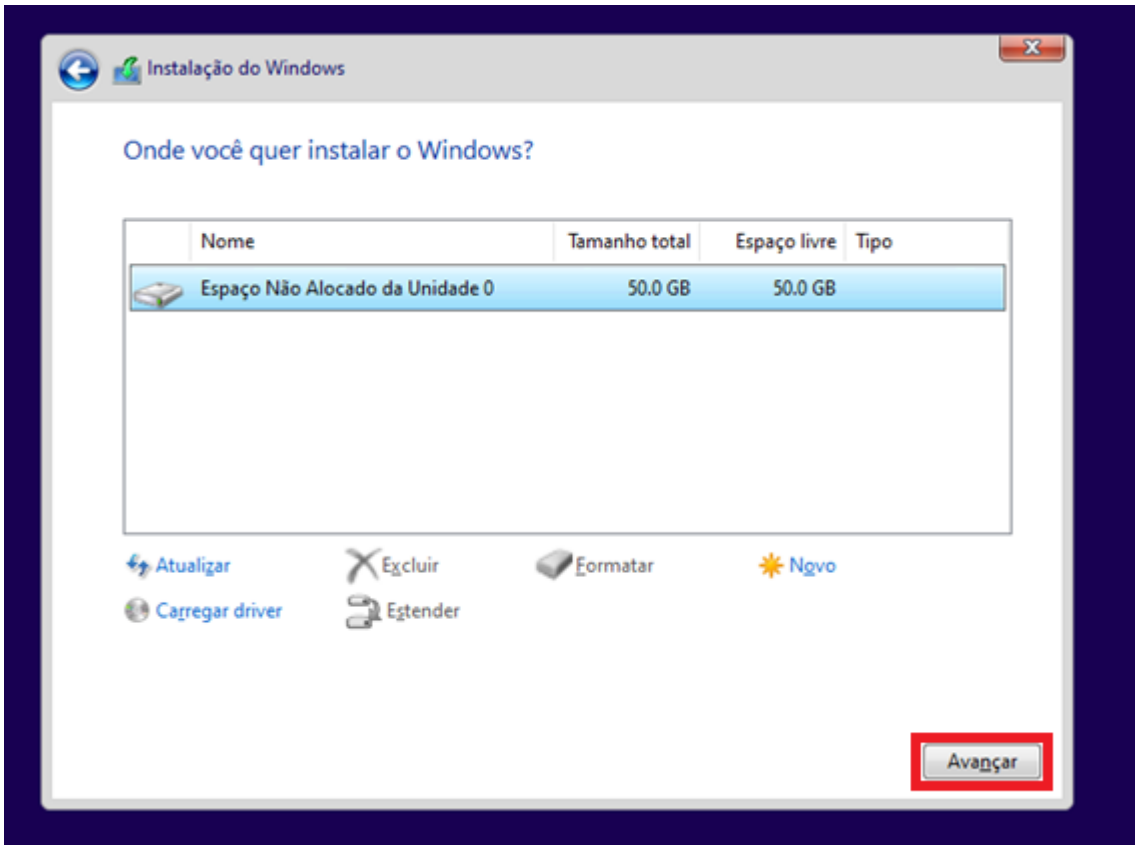
Fonte: Elaborada pela Autora.

Figura 31 – Instalação do Sistema Operacional Windows



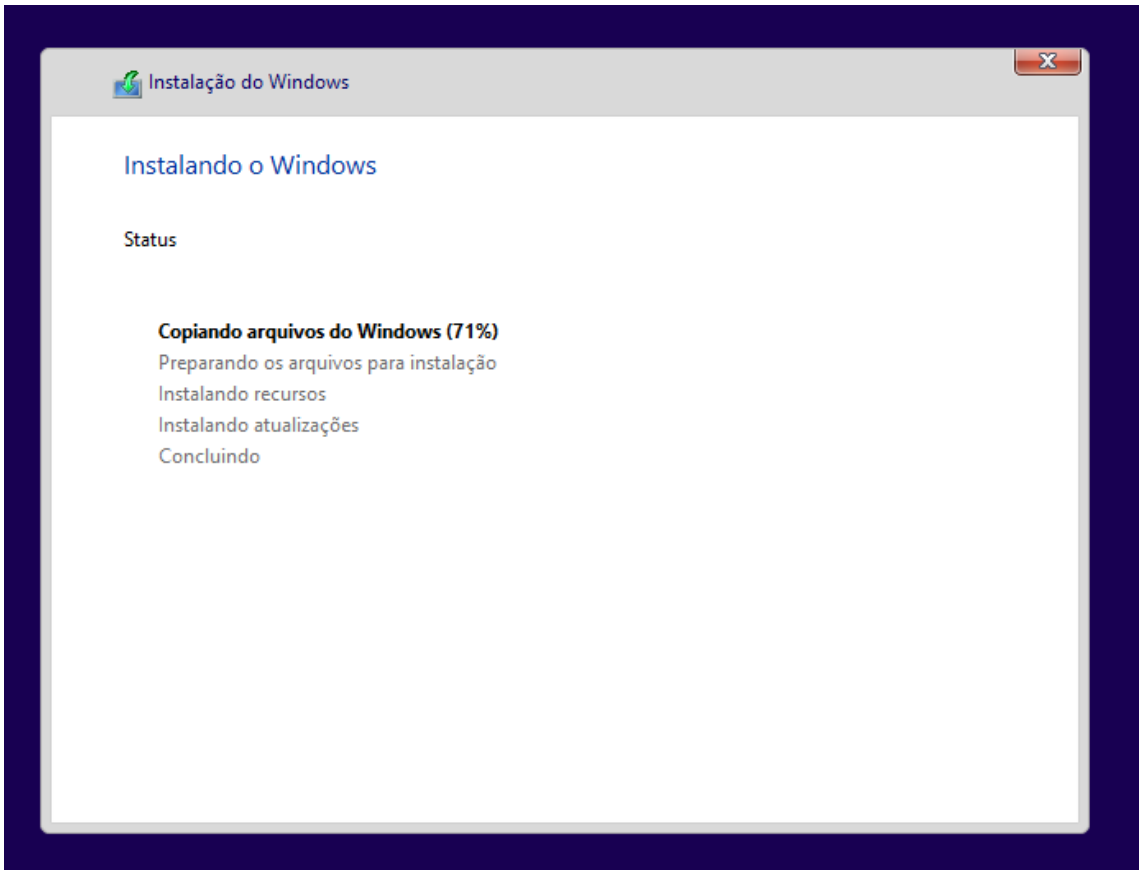
Fonte: Elaborada pela Autora.

Figura 32 – Instalação do Sistema Operacional Windows



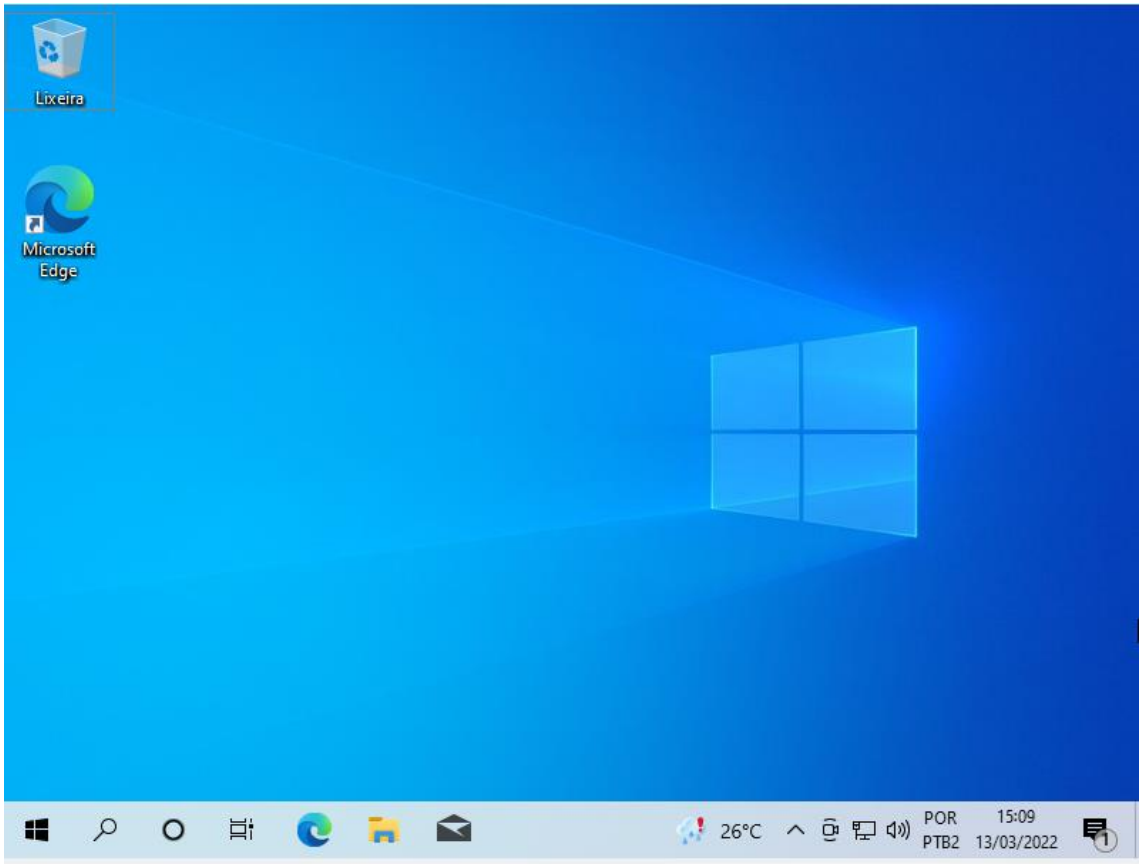
Fonte: Elaborada pela Autora.

Figura 33 – Instalação do Sistema Operacional Windows



Fonte: Elaborada pela Autora.

Figura 34 – Instalação do Sistema Operacional Windows



Fonte: Elaborada pela Autora.