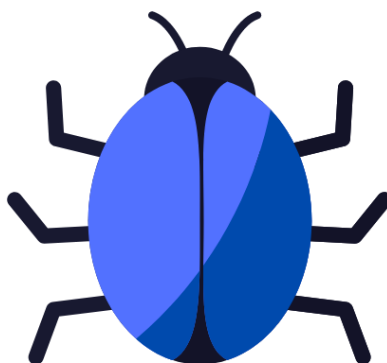


DICAS PARA CRIAR SUA SANDBOX PARA ANÁLISE DE ARTEFATOS MALICIOSOS



Elaborado por:

CAIQUE BARQUETA

Digital Forensic Analytic and Incidente Responder

LinkedIn: <https://www.linkedin.com/in/caique-barqueta-635613129/>

Este guia foi elaborado para auxiliar os profissionais na área de Segurança da Informação/ Cibersegurança que atuam como Analistas de Segurança da Informação, times de SOC, Peritos Forenses, estudantes e entusiastas na área de análise de artefatos maliciosos.

Caso venha ter dúvida acerca de algum conteúdo, fico a disposição para ajudá-lo(a) podendo ser realizado o contato por meio do meu LinkedIn.

Poderá ser realizado análises tanto iniciais de forma estática e dinâmica por meio da utilização da referida VM.

INICIANDO

Devido à grande propagação de arquivos e artefatos maliciosos que acabam por se espalhar de vários métodos, como por exemplo por meio de conexões USB, e-mails phishing, recrutamento de colaboradores internos entre outros métodos visando prejudicar tanto o ambiente corporativo quanto privado, se faz necessário realizar a checagem dos referidos arquivos antes de ser executado ou aberto em ambiente real, visando sempre identificar se aquele dado arquivo trata-se de algo potencialmente malicioso ou não.

No decorrer desta cartilha, comento também um pouco sobre as ferramentas e técnicas de análise de malware, tanto estática quando dinâmica, as quais são empenhadas para encontrar artefatos maliciosos. Lembrando que não irei aprofundar em cada ferramenta, é breve, para fins de auxílio.

O QUE É UMA SANDBOX?

No mundo de ciber, a utilização da Sandbox se dá por um ambiente que pode ser totalmente isolado e que se parece com ambientes operacionais do usuário final, ou seja, é igual a uma máquina física que você tem em casa ou no escritório, porém de forma virtual, e com isto auxilia na execução de arquivos suspeitos visando principalmente para conhecer o comportamento caso seja suspeito.

REQUERIMENTOS E DICAS PARA INSTALAÇÃO

Visando construir uma Sandbox, recomendo que seja definido alguns requisitos de hardware ou software, porém vale salientar que varia de acordo com seu ambiente e o que você tem de hardware e software, mas o contexto aqui aplicado é o mesmo, independente do desempenho da Máquina Virtual escolhida.

DICAS DE REQUISITOS:

CPU de 2,4 GHz mínimo (ou superior)

4 ou 6GB de RAM (ou superior)

100 GB de espaço livre no disco rígido (ou superior)

Sistema Operacional do Host (Linux, MacOS, Win10...)

Instalação ou da VMWare ou VirtualBox

Sistema Operacional da Sandbox (Win7, 8, 10...)

Lembrando, este são algumas dicas, faça adaptação de acordo com seu ambiente! Abaixo mostro como realizar a montagem de uma Máquina Virtual Windows 10 64 bits no ambiente do VirtualBox.

MONTANDO UMA MÁQUINA VIRTUAL NO VIRTUALBOX

Faça o download da imagem ISO, (neste caso escolhi do Windows 10).

<https://www.microsoft.com/pt-br/software-download/windows10?ranMID=42431>

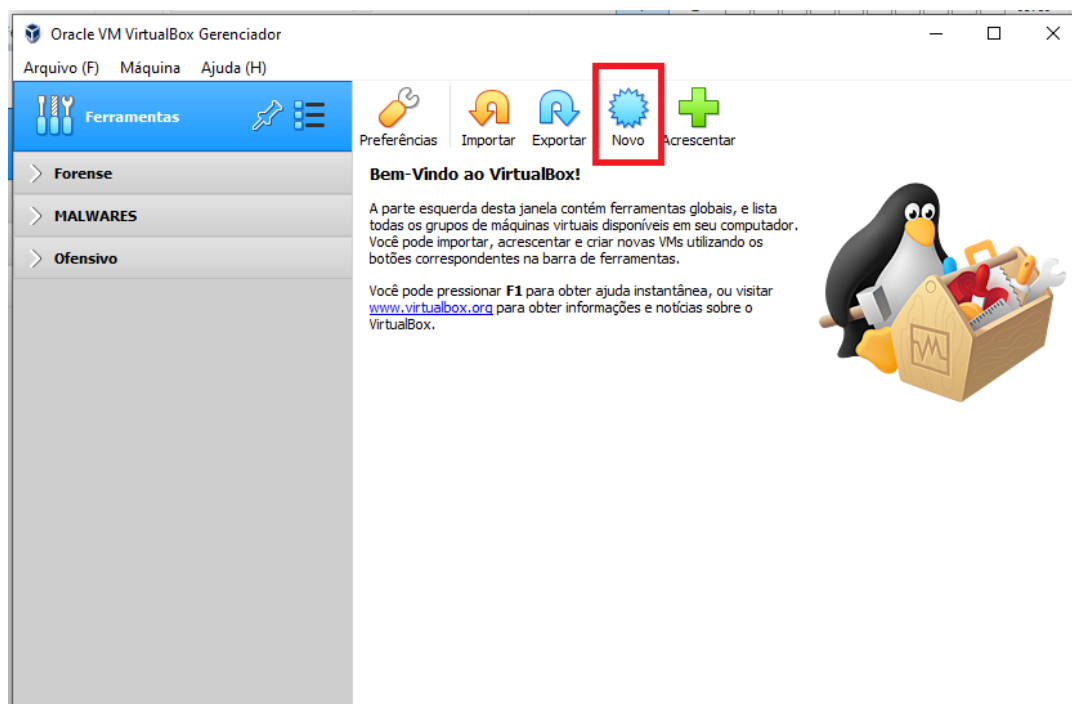
Baixe o VirtualBox

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

Faça o download da extensão também caso venha precisar.

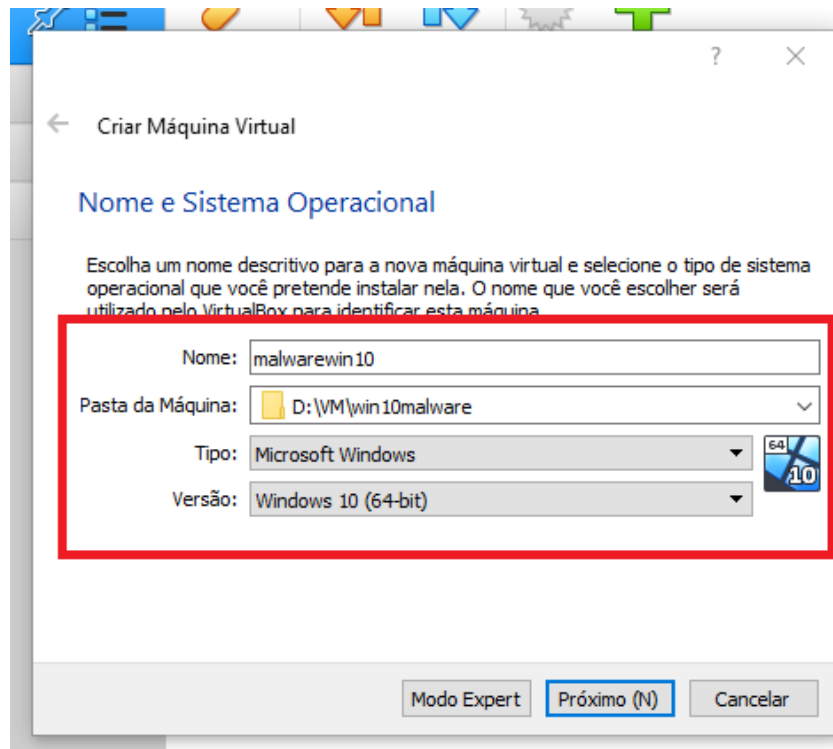
https://download.virtualbox.org/virtualbox/6.1.32/Oracle_VM_VirtualBox_Extension_Pack-6.1.32.vbox-extpack

Após baixar e instalar o VirtualBox e sua extensão, clique na opção “Novo”.

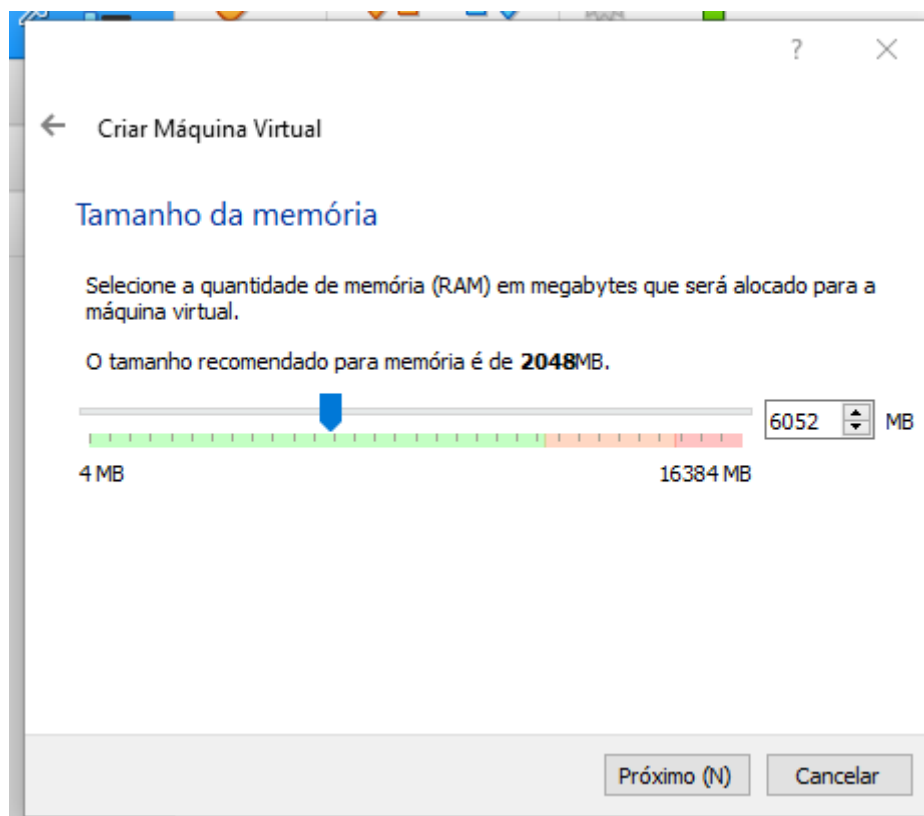


Obs: Percebam que eu já tenho algumas Máquinas Virtuais, caso não tenha, a coluna na esquerda está limpa.

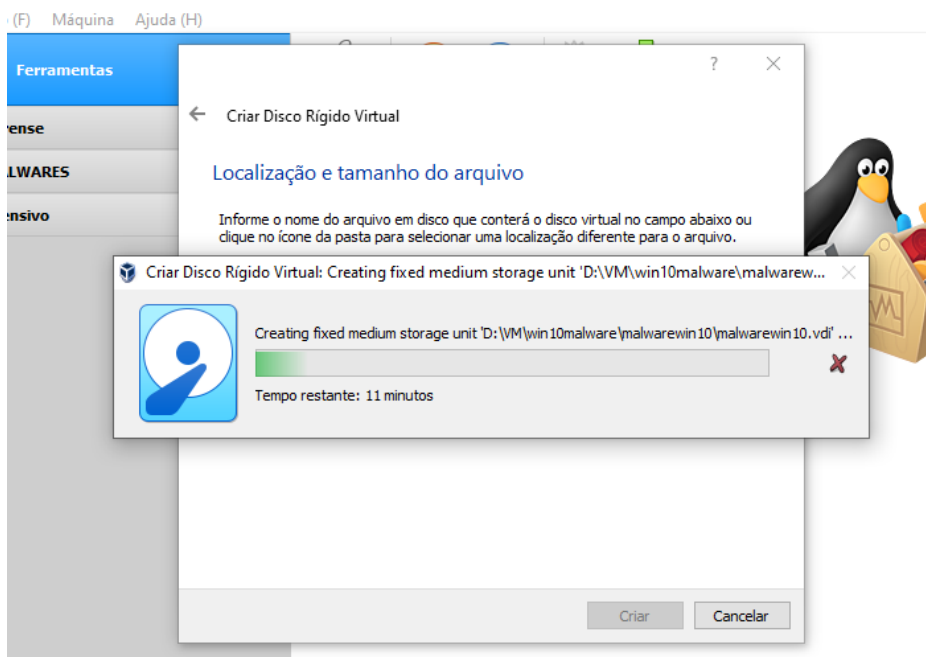
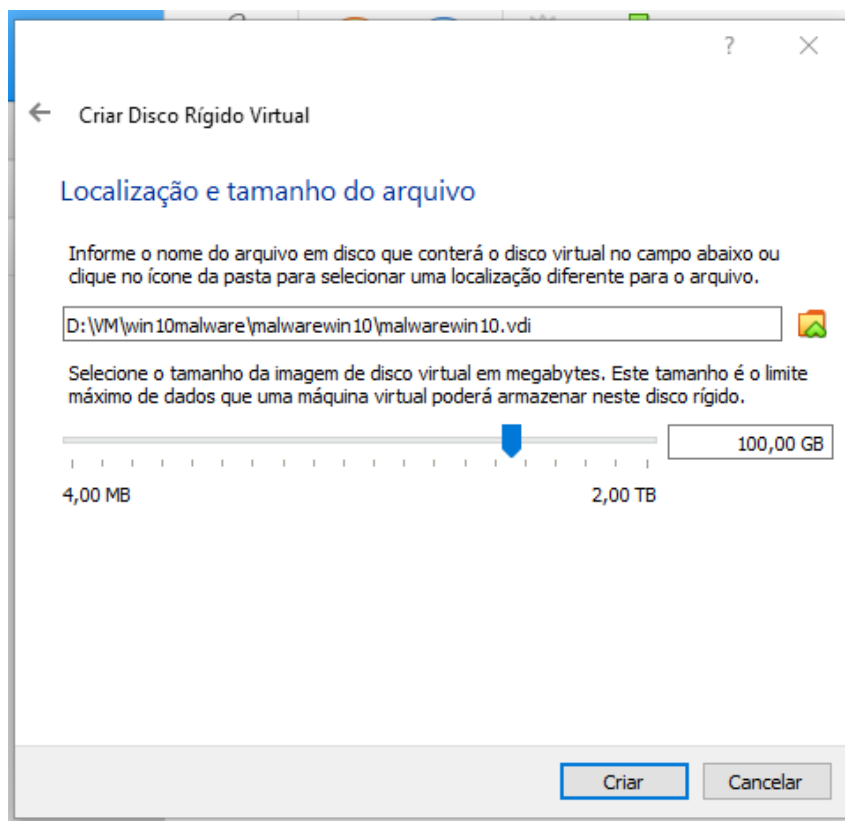
Após clicar em Novo, comece a realizar a configuração de sua preferência de acordo com sua realidade!



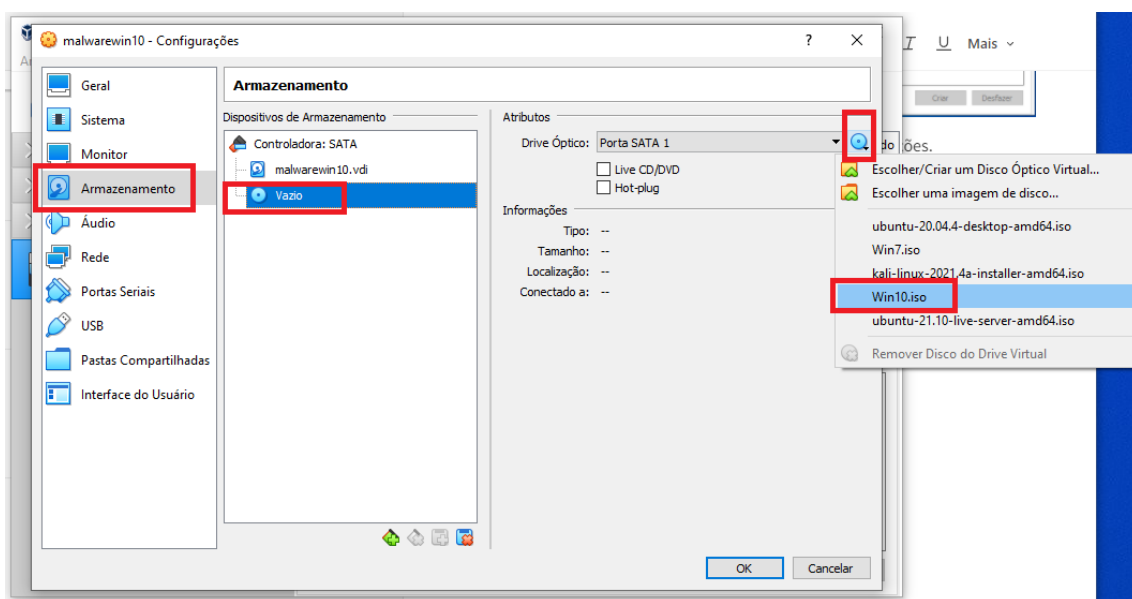
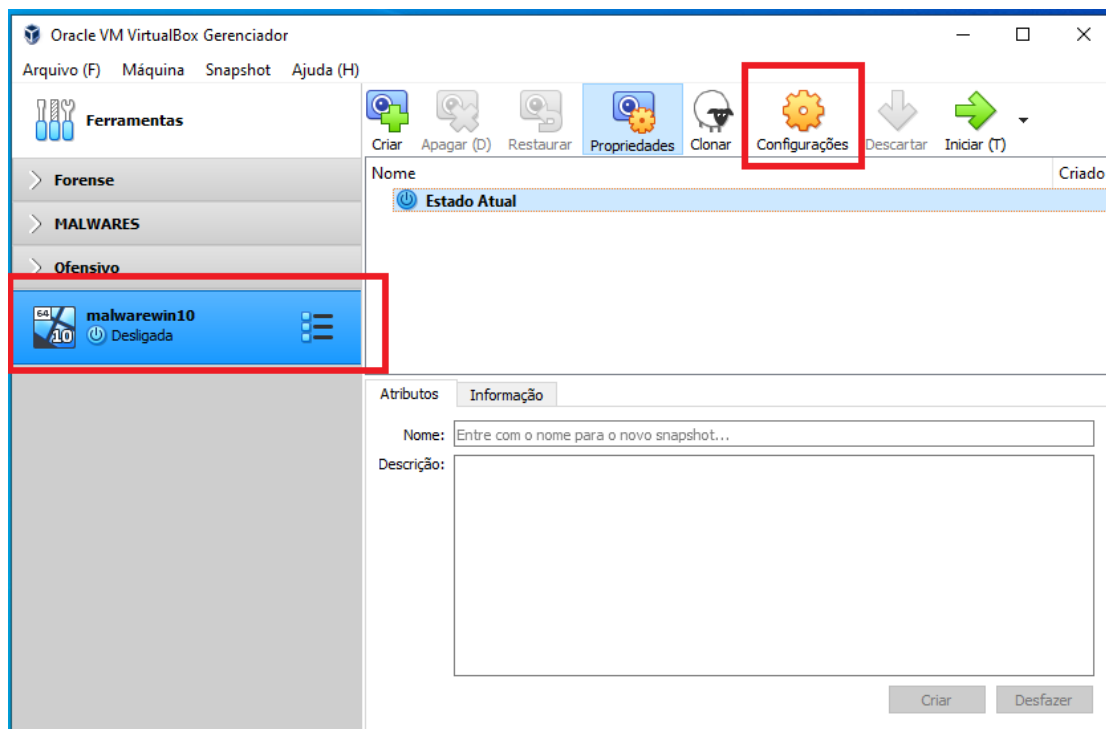
Escolha o tamanho de Memória a ser utilizado pela SandBox.

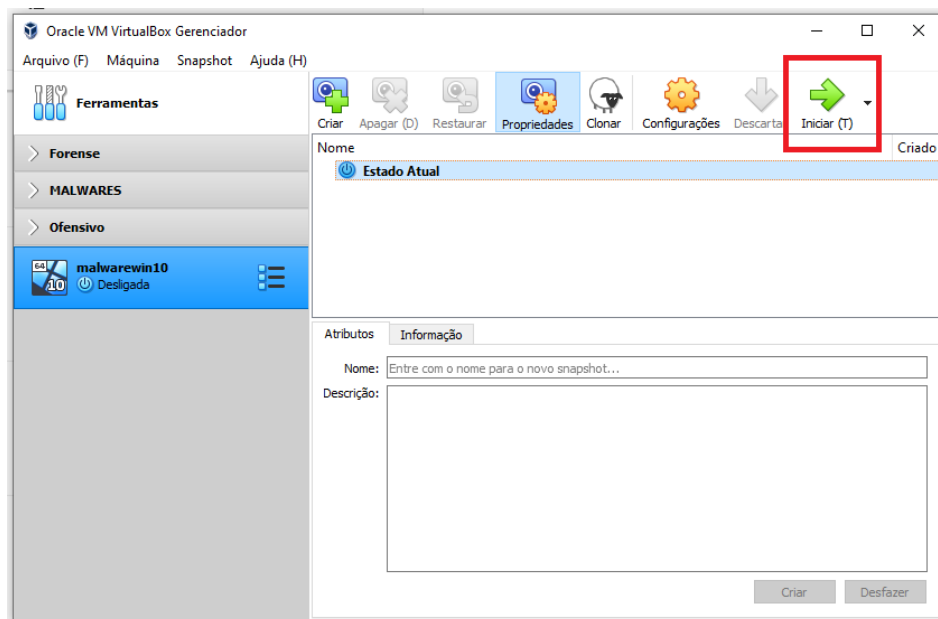


Escolha também o espaço em disco desejado para alocar! Aqui salientei que é bom montar uma com 100GB, você pode montar ela dinamicamente alocada ou fixa, neste caso montei de modo fixo.

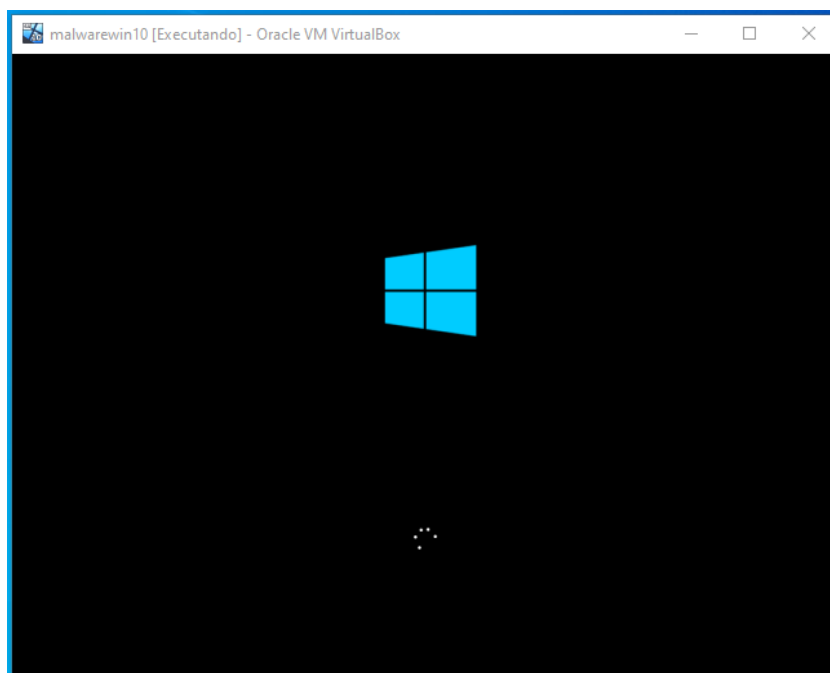


Finalizado a criação da máquina, precisa realizar a utilização da imagem ISO para instalação do Sistema Operacional, para isto selecione a Máquina Virtual criada, vá em Configurações, Armazenamento, na seção de Dispositivos de Armazenamento clique no ícone do CD e em seguida selecione a ISO que utilizará para instalar o Sistema Operacional. Após selecionar, inicie a VM.



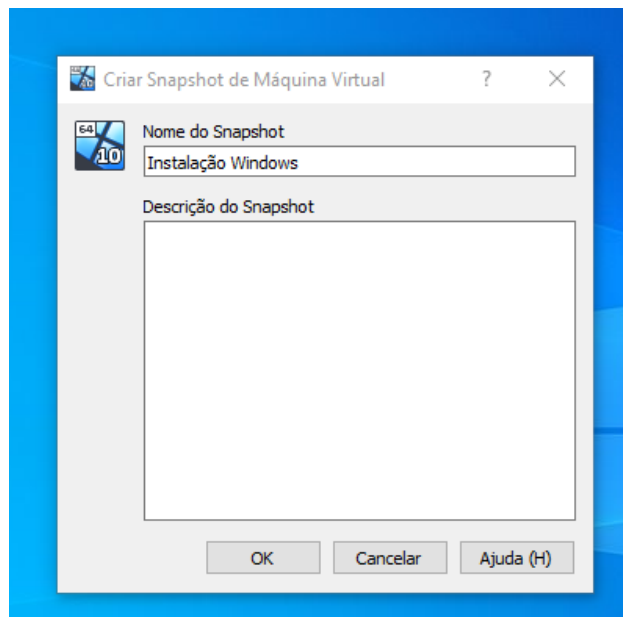


Em seguida, a VM será carregada e inicializada a instalação do Sistema Operacional.



Um tópico superimportante sobre a VM é que com ela você pode realizar a criação de um Snapshot, ou seja, após a conclusão da instalação do Sistema Operacional, crie uma Snapshot a qual caso ocorra algum erro na preparação será possível reverter ao estado do SnapShot tirado! Isso é

muito útil pois caso venha analisar o comportamento do malware poderá realizar Snapshot para capturar e retornar seu ambiente!



Após a instalação existe a possibilidade de realizar a instalação de um kit de ferramentas por meio da FLARE-VM. Este projeto está disponível no GitHub e trás muitas ferramentas que utilizamos para analisar arquivos maliciosos, caso queira instalar aplicativo por aplicativo, fique a vontade. A minha dica é, instale a Flare, ela já vem com muita coisa e você só precisa acrescentar algumas específicas.

Lembrando que agora todas as operações serão realizadas na VM criada e não na máquina Host, logo para realizar o download da Flare, acesse:

<https://github.com/mandiant/flare-vm>

Após o download do arquivo, desabilite o sistema de segurança do Windows, descompacte-o arquivo relacionado a Flare.

Abra o PowerShell em modo Administrador e vá até a pasta que realizou a descompactação da flare.

```
Windows PowerShell
PS C:\Users\Perito\Desktop\flare-vm-master> dir

Diretório: C:\Users\Perito\Desktop\flare-vm-master

Mode                LastWriteTime         Length Name
----                -
d-----          22/10/2021   23:13             flarevm.config.flare
d-----          22/10/2021   23:13             flarevm.installer.flare
d-----          22/10/2021   23:13             flarevm.win10.config.fireeye
d-----          22/10/2021   23:13             flarevm.win10.installer.fireeye
d-----          22/10/2021   23:13             flarevm.win10.preconfig.fireeye
d-----          22/10/2021   23:13             550 .gitattributes
d-----          22/10/2021   23:13             469 .gitignore
d-----          22/10/2021   23:13            13129 flarevm.png
d-----          22/10/2021   23:13            16132 install.ps1
d-----          22/10/2021   23:13             9192 LICENSE.txt
d-----          22/10/2021   23:13            26850 packages.csv
d-----          22/10/2021   23:13             5296 profile.json
d-----          22/10/2021   23:13            17570 README.md

PS C:\Users\Perito\Desktop\flare-vm-master>
```

Desbloqueie o arquivo de instalação da Flare.

> **Unblock-File .\install.ps1**

```
PS C:\Users\Perito\Desktop\flare-vm-master> Unblock-File .\install.ps1
```

Em seguida dê o comando **"Set-ExecutionPolicy Unrestricted"**.

```
PS C:\Users\Perito\Desktop\flare-vm-master> Unblock-File .\install.ps1
PS C:\Users\Perito\Desktop\flare-vm-master> Set-ExecutionPolicy Unrestricted

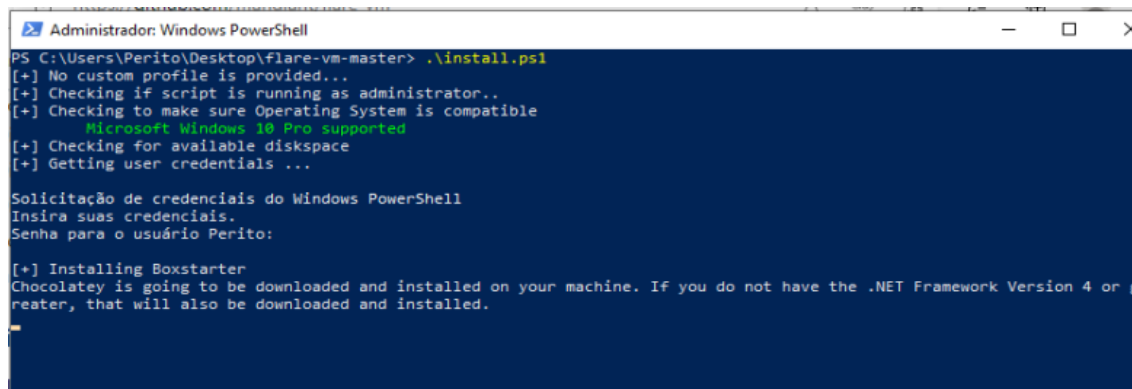
Alteração da Política de Execução
A política de execução ajuda a proteger contra scripts não confiáveis. A alteração da política de execução pode implicar exposição aos riscos de segurança descritos no tópico da ajuda about_Execution_Policies em https://go.microsoft.com/fwlink/?LinkID=135170. Deseja alterar a política de execução?
[S] Sim [A] Sim para Todos [N] Não [T] Não para Todos [U] Suspender [?] Ajuda (o padrão é "N"): S
PS C:\Users\Perito\Desktop\flare-vm-master>
```

Posteriormente a isto, instale e execute o arquivo **.\install.ps1**.

```
Administrador: Windows PowerShell
PS C:\Users\Perito\Desktop\flare-vm-master> .\install.ps1
```

Em seguida, caso tenha setado senha para a VM, ele irá requisitar a referida senha do usuário, forneça-a e deixe instalando, vá tomar um café, um chá, comer uns pãezinhos que vai demorar.

Lembrando que a rede poderá ser deixada em modo NAT ou Bridge por enquanto, visto que a Flare irá realizar o download de arquivos para sua instalação.



```
Administrador: Windows PowerShell
PS C:\Users\Perito\Desktop\flare-vm-master> .\install.ps1
[+] No custom profile is provided...
[+] Checking if script is running as administrator..
[+] Checking to make sure Operating System is compatible
    Microsoft Windows 10 Pro supported
[+] Checking for available disk space
[+] Getting user credentials ...

Solicitação de credenciais do Windows PowerShell
Insira suas credenciais.
Senha para o usuário Perito:

[+] Installing Boxstarter
Chocolatey is going to be downloaded and installed on your machine. If you do not have the .NET Framework Version 4 or greater, that will also be downloaded and installed.
```

Após o término da instalação, você poderá acrescentar ferramentas para incrementar mais ainda a sua VM para análise. A dica que deixo é que deixe-a parecendo com um ambiente realmente normal, instale aplicativos do tipo Adobe Reader, Office... programas que usuários contém em máquina, visto que existem malwares que buscaram por tais informações visando identificar se estão sendo executados em ambiente virtual ou não.

Adiante, deixo a série de ferramentas e “um roteiro” para seguir de acordo com a análise que estiver realizando e faço um pouco sobre cada ferramenta para que você possa entender.

Por fim, não se esqueça, terminou a instalação da Flare-VM faça uma SNAPSHOT!

DICAS DE FERRAMENTAS UTILIZADAS EM ANÁLISE

ANÁLISE ESTÁTICA

VIRUSTOTAL: É uma ferramenta web disponível em <https://virustotal.com> a qual visa classificar e identificar por meio de assinaturas e demais informações do arquivo por diversos anvírus. O VirusTotal é muito utilizado para classificar o tipo de arquivo malicioso ou família, pois pode se tratar de Ransomware, Spys, Key, Downloaders etc.

Existe ainda a possibilidade da utilização da ferramenta **YARA**, a qual realiza o mesmo trabalho do VirusTotal, e que pode ser acessada em: <https://virustotal.github.io/yara/> e existem ainda alguns repositórios em: <https://github.com/Yara-Rules/rules>

EXEInfo e Detect It Easy, as quais são ferramentas em GUI utilizada para analisar informações do cabeçalho PE, sendo que em sua utilização poderá ser verificado informações como importações realizadas, strings, se o arquivo está empacotado ou não e identificar mais dados.

EXEInfo: <https://exeinfo-pe.en.uptodown.com/windows>

Detect It Easy (DiE): <https://github.com/horsicq/Detect-It-Easy>

UPX (Descompactador): existem arquivos maliciosos que poderão estar compactados com UPX, logo também existe a ferramenta que faz a descompactação e output do arquivo escondido.

UPX: <https://upx.github.io/>

> upx -d <nomedoarquivomalicioso> -o <arquivosaída>

Ferramenta para Cálculo de Hash: muito importante para que sejam geradas IOCs acerca do arquivo, visto que atualmente utilizado o algoritmo md5 e sha256 para identificação dos referidos arquivos maliciosos, como

existem diversas calculadoras de hash, poderá usar de sua preferência, mas a título de exemplo existem, **FSUM**, **HashMyFiles...**

PEstudio: Ferramenta que foi desenvolvida especificamente para realizar a análise estática de arquivos potencialmente maliciosos, pois conforme o DIE, possui função de busca de strings, imports, consulta ao VirusTotal entre outras.

PEstudio: <https://www.winitor.com/features/>

FERRAMENTAS DE ANÁLISE DINÂMICA:

ProcessHacker: Ferramenta utilizada para monitorar os processos que estão em execução pelo Sistema, muito útil para verificar quais processos criados e identificar PID destes.

FAKENET: Ferramenta utilizada para auxiliar na simulação de uma rede para que o arquivo malicioso interaja com o Host remoto e continue em execução, permitindo que você observe a atividade de rede do malware dentro da VM.

Fakenet: <https://www.fireeye.com/services/freeware/fakenet-ng.html>

RegShot: Ferramenta utilizada para monitoramento da integridade do registro e do sistema de arquivos do Sistema Operacional, você pode realizar 1 Shot antes da execução e depois o 2 Shot pós execução e compará-lo, verificando-os registros alterados e informações.

RegShot: <https://sourceforge.net/projects/regshot/>

ProcMon: Realiza o registro de atividade do sistema em tempo real, como criação de processos, escritas e criação de novos arquivos, conexões de redes e ainda possui uma vasta possibilidade de realizar filtragem em busca de informações.

ProcMon: <https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>

Autoruns: Ferramenta muito útil da Microsoft, a qual verifica caminhos de persistência do Sistema Operacional, como chave /Run, tarefas criadas, serviços entre outros, podendo este ser comparado pós execução do arquivo malicioso.

Autoruns: <https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns>

FileGrab: Ferramenta que monitora o sistema de arquivos do Windows, realizando a captura de arquivos recém criados e gerando cópia destes arquivos para outro local, podendo ser na mesma VM ou via Rede.

FileGrab: <https://sourceforge.net/projects/filegrab/>

Estes foram alguns das ferramentas que deixo como resumo, existem outras, caso tenha instalado a Flare, lá vem com todas! Basta pesquisar que encontrará as mesmas na VM, pois bem agora que dei a introdução básica, vamos simular uma análise para melhor entender.

Lembre-se, faça **SnapShot** após a instalação das ferramentas e ambiente completo para que seja revertido após execução do malware.

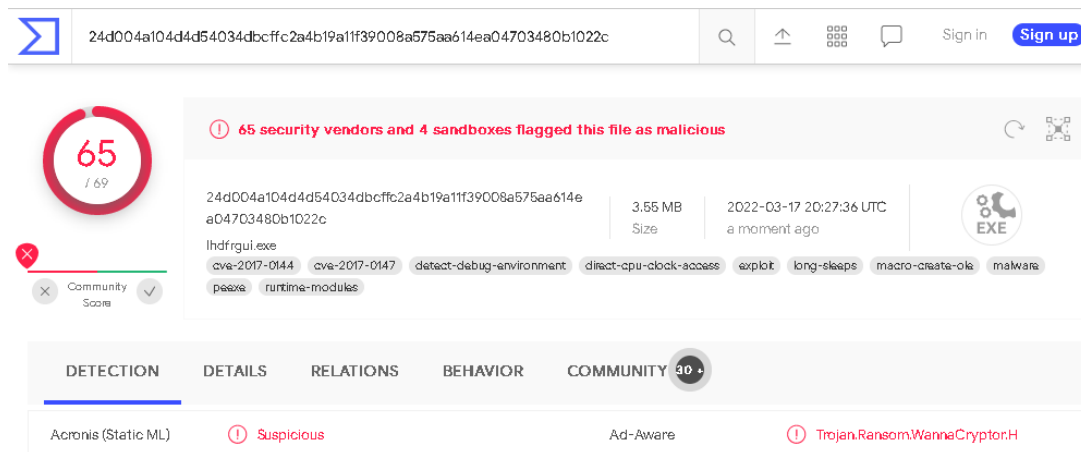
PREPARAÇÃO PARA ANÁLISE DINÂMICA

Faça o SNAPSHOT!

Configure a rede para modo **"HOST-ONLY"** e isole a VM impedindo o recurso de Arrastar/Soltar e Copiar e Colar para dentro da VM.

SIMULAÇÃO DE ANÁLISE

Com o arquivo potencialmente malicioso, submeti o mesmo para análise através do VirusTotal, o qual identificou 65 de 69 antivírus como arquivo malicioso.



24d004a104d4d54034dbccfc2a4b19a11f39008a575aa614ea04703480b1022c

65 / 69

65 security vendors and 4 sandboxes flagged this file as malicious

lhdfgui.exe

3.55 MB Size

2022-03-17 20:27:36 UTC a moment ago

EXE

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30+

Acronis (Static ML) Suspicious

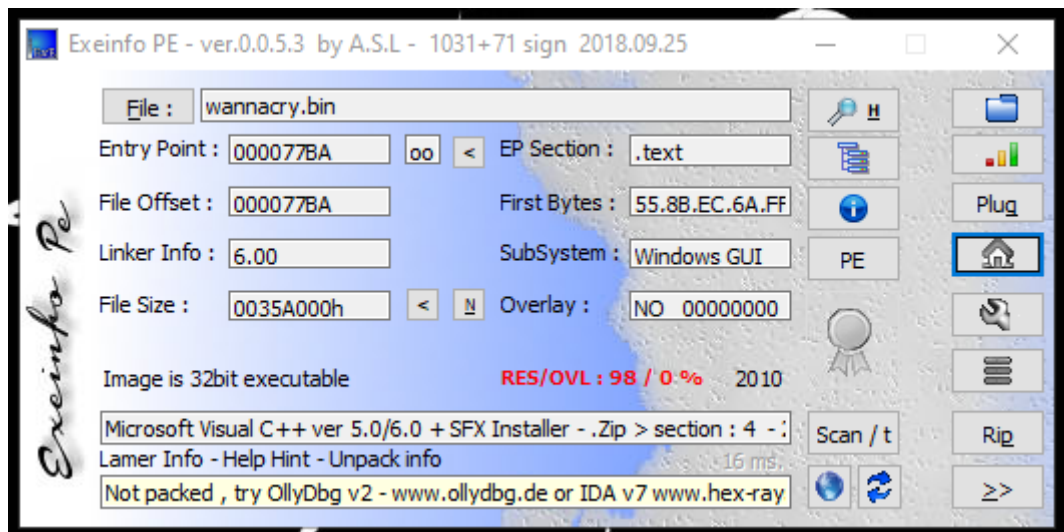
Ad-Aware Trojan.Ransom.WannaCryptor.H

Aqui vale lembrar, que se o arquivo for potencialmente confidencial, deverá ser analisado realmente a necessidade de submetê-lo para análise do VirusTotal.

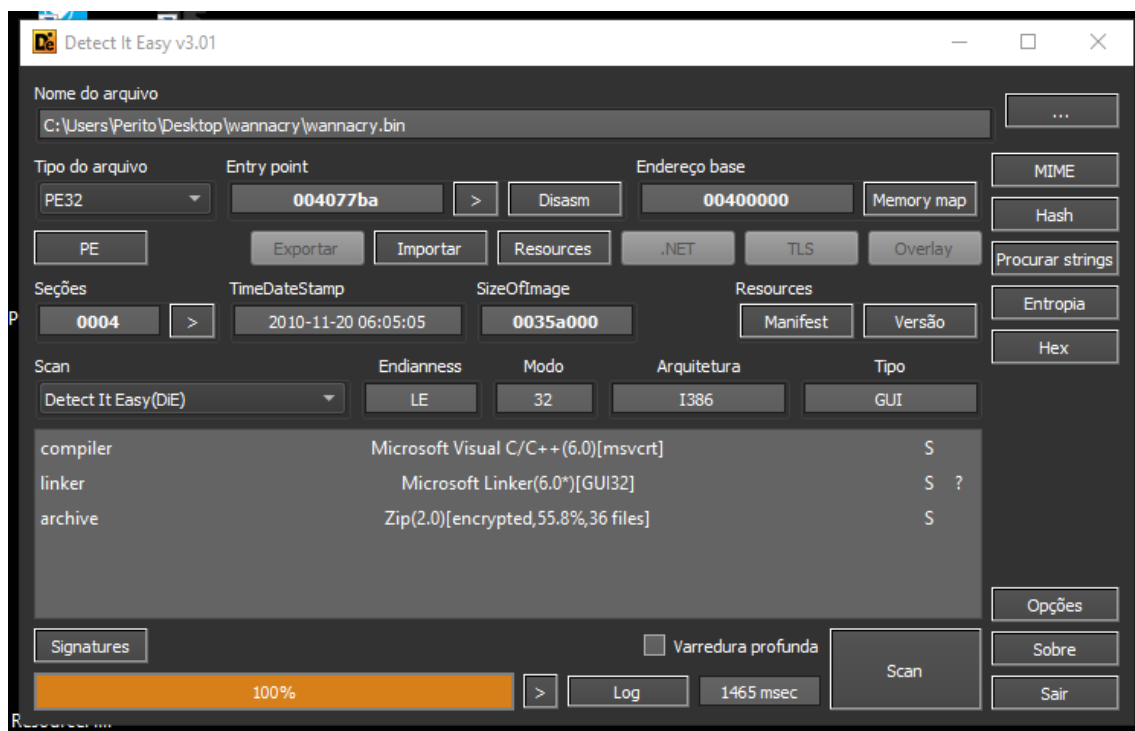
O VírusTotal irá trazer informações do referido arquivo, como assinaturas e regras Yara para identificá-lo.

Basic Properties ⓘ	
MD5	db349b97c37d22f5ea1d1841e3c89eb4
SHA-1	e889544aff85ffaf8b0d0da705105dee7c97fe26
SHA-256	24d004a104d4d54034dbccfc2a4b19a11f39008a575aa614ea04703480b1022c
Vhash	036046651d6570b8z201cpz31zd025z
Authentihash	1646cad4fe91337460de0d4c2c5451095023e74bdab331642aaca12647b72f46
Imphash	9ecee117164e0b870a53dd187cdd7174
Rich PE header hash	09c088bc95bf88e6f4df4d6ca904611b
SSDEEP	98304:wDqPoBhz1aRxcSUDk36SAEdhvxWa9P693R8yAVp2g3R:wDqPe1Cxcxk3ZAEUadzR8yc4gB
TLSH	T1B70633A8962DA1BCF0050DB044928557EBFB3C57B7BA5A2FCF4045660D43B6F9BC0E61
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (38.8%)
TrID	Microsoft Visual C++ compiled executable (generic) (20.5%)
TrID	Win64 Executable (generic) (13%)
TrID	Win32 Dynamic Link Library (generic) (8.1%)
TrID	Win16 NE executable (generic) (6.2%)
File size	3.55 MB (3723264 bytes)
PEID packer	Microsoft Visual C++
Cyren packer	rsrc

Em seguida, vamos analisar o cabeçalho do PE com as ferramentas EXEInfo PE e DIE.

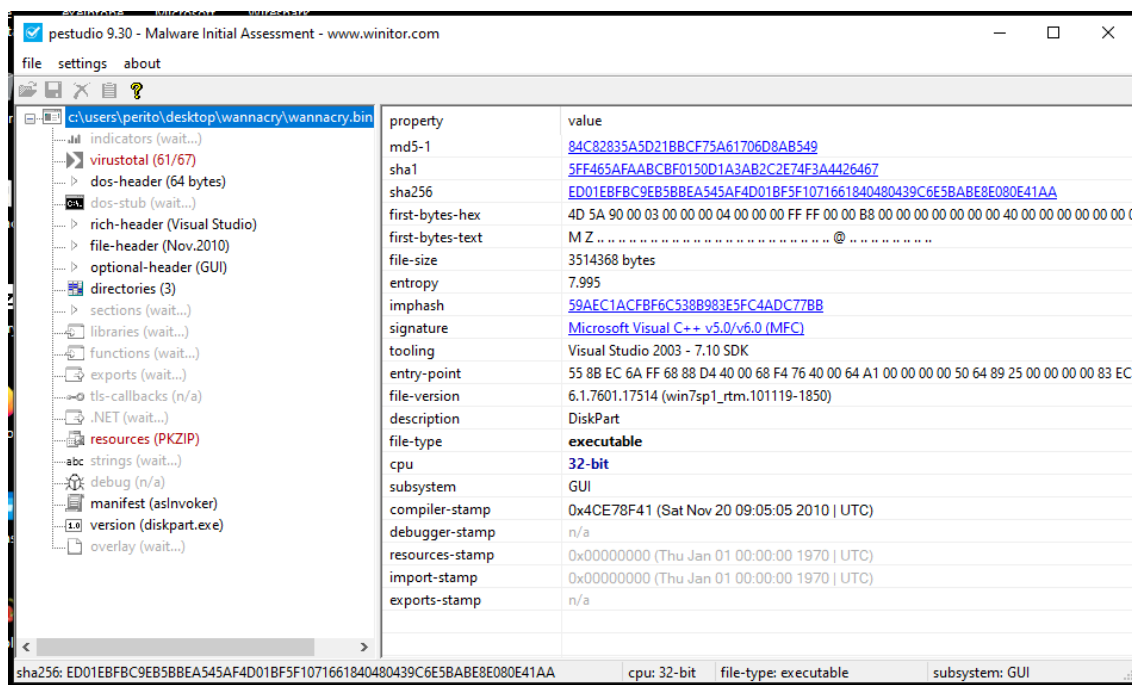


(Análise com o EXEInfo)



(Análise com o DIE)

Análise com a ferramenta PEStudio, conforme afirmei acima, esta ferramenta é muito útil para concentrar algumas informações do malware a ser analisado.



(Ferramenta PEStudio).

Resumo das principais informações:

Virustotal: envia um hash do arquivo para verificar o resultado.

Cabeçalho do arquivo: Contém a data de criação do arquivo e o idioma do computador do autor.

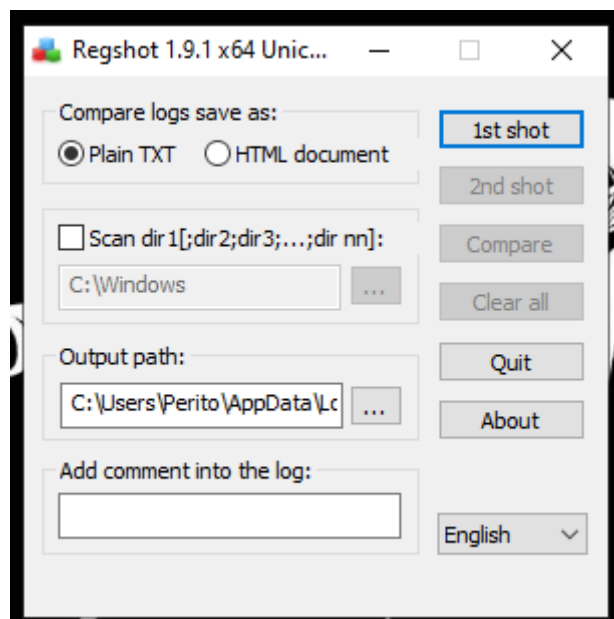
Importações: Apresenta uma lista de funções e bibliotecas que estão na lista negra que são potencialmente usados por malware.

Strings: Lista todas as strings suspeitas encontradas no arquivo analisado.

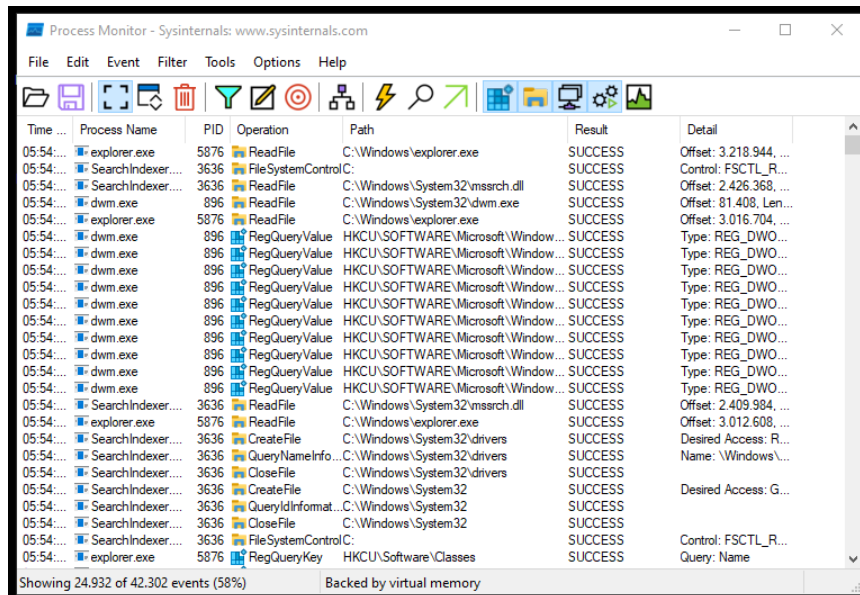
Antes da execução do arquivo, vamos habilitar da FakeNet, ele irá apresentar todos os serviços de internet, como HTTPS, DNS, SMTP...



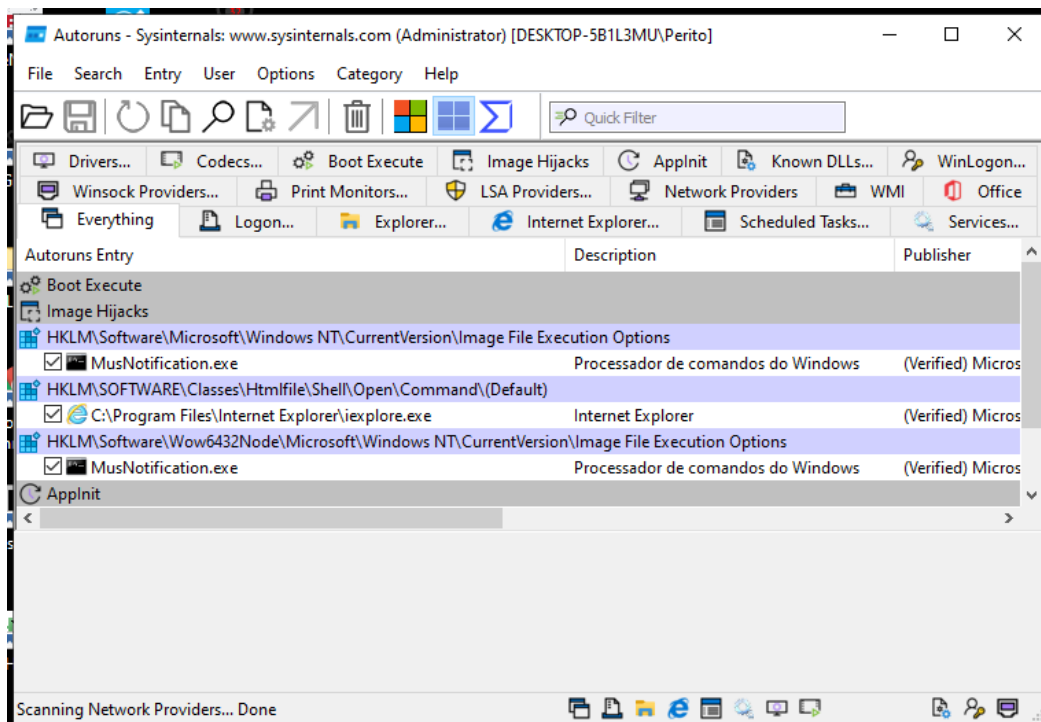
Realize a captura de 1 Shot com a ferramenta RegShot. Não esqueça de depois de executar o malware realizar o 2 shot para compará-lo e verificar as alterações do sistema.



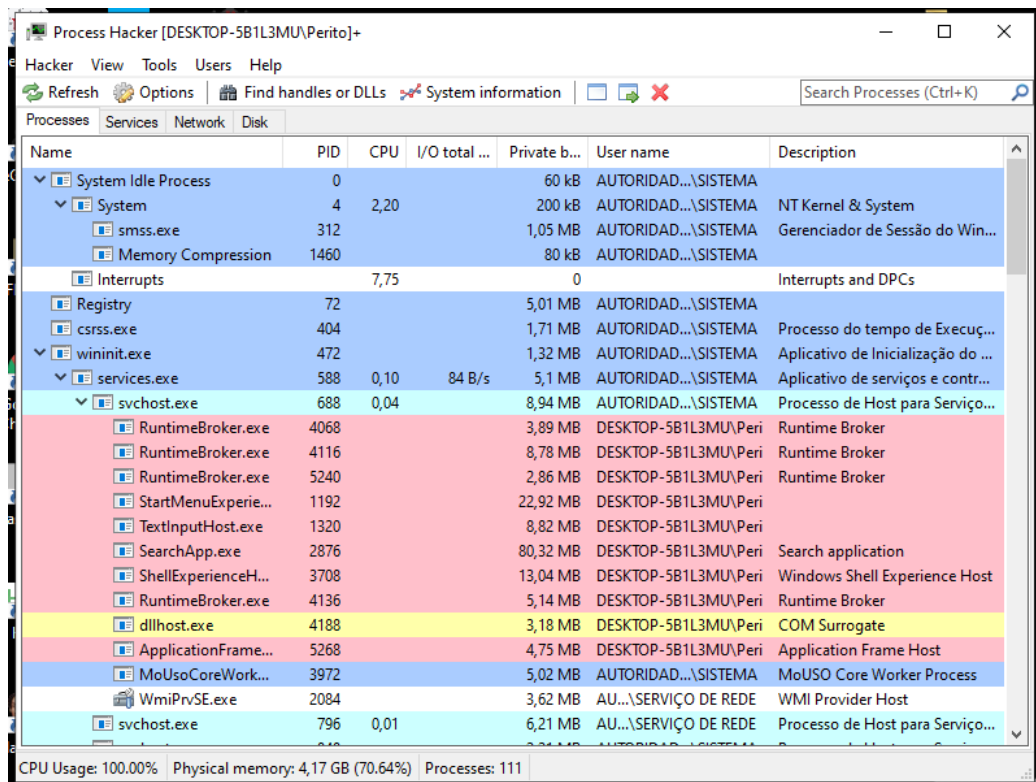
Abra o ProcMon e deixe-o em segundo plano, ele irá capturar conforme falado todos os registros de processos, criação ou exclusão de arquivos e etc...



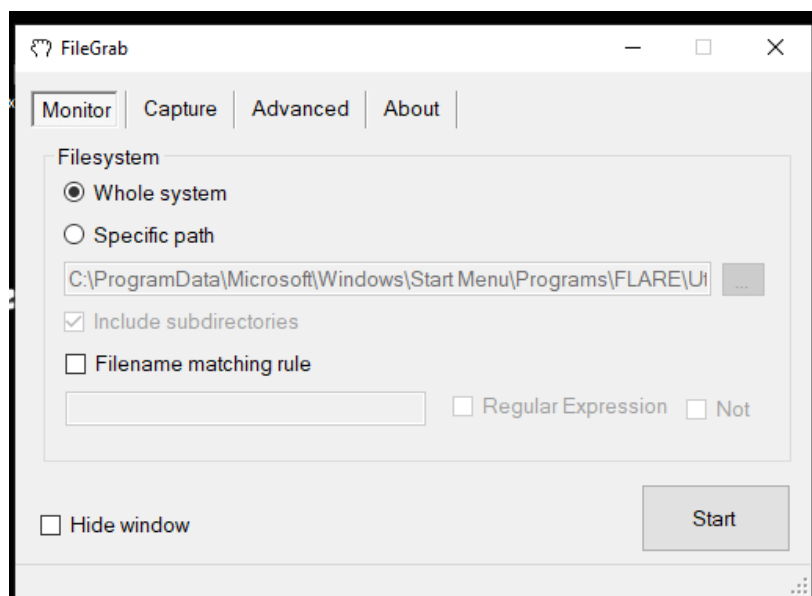
Realize a abertura do Autoruns e salve um backup dos registros, o qual poderá ser utilizado posteriormente para realizar a comparação.



Abra o ProcessHacker e deixe-o executando, pois será possível verificar o PID criado pelo processo do arquivo malicioso.



Poderá ainda habilitar o FileGrab e especificar a pasta desejada para realizar o despejo dos arquivos criados pelo arquivo malicioso.



FINALIZAÇÃO

Como afirmei acima, como não se trata de cartilha voltada para análise de determinado artefato, mas sim para **auxiliar na montagem de uma Máquina Virtual e demais ferramentas utilizadas**, onde podemos concluir que a VM é uma das grandes ferramentas que atualmente os analistas e peritos possuem para realizar a análise de arquivos considerados potencialmente ou maliciosos.

Caso restem dúvidas sobre algum ponto sinalizado aqui nesta cartilha, meu canal de comunicação pelo LinkedIn e Telegram estão disponíveis!

Por fim, a última recomendação que deixo é, compartilhe conteúdo, compartilhe conhecimento! Quem compartilha este tipo de conteúdo acaba adquirindo muito mais!

Espero poder ter ajudado, e lembre-se, antes de executar, SNAPSHOT e Host-Only!

