

ANÁLISE DE MALWARE STARTER

Caique Barqueta



SOBRE A ACADEMIA DE FORENSE DIGITAL

A AFD – “Academia de Forense Digital”

Nasceu em 2016 com o objetivo de apoiar o desenvolvimento e a boa condução da Justiça em nosso país, através da educação e do compartilhamento de conhecimentos na área de Forense Digital, possibilitando também que profissionais e estudantes ingressassem e pudessem alcançar melhor desenvolvimento em suas carreiras.



Atualmente estamos entre as maiores instituições de Ensino na área de Forense Digital



- Mais de mil estudantes formados
- 16 treinamentos na área
- 3.5 mil inscritos no canal do YouTube e 230 vídeos publicados



Organizadores do AFD Summit
**Nós somos ESPECIALISTAS em
Forense Digital**

VANTAGENS EM FAZER PARTE!

Na matrícula do treinamento você recebe:

- 1 ano de acesso em nossa Plataforma
- Acesso à versão gravada do respectivo treinamento
- Livre acesso às turmas ao vivo do respectivo treinamento
- MeetUps
- Grupos de Discussão Exclusivos
- Garantia de 7 dias
- 1 ano de assinatura AFD Stream





VANTAGENS EM FAZER PARTE!

- AFD Stream
- Mini Treinamentos
- Palestras Exclusivas
- AFD Case Files CTF
- AFD Tech
- AFD Summit Online
- Descontos na S.O.S Peritos
- Descontos em Parceiros

WHOAMI?

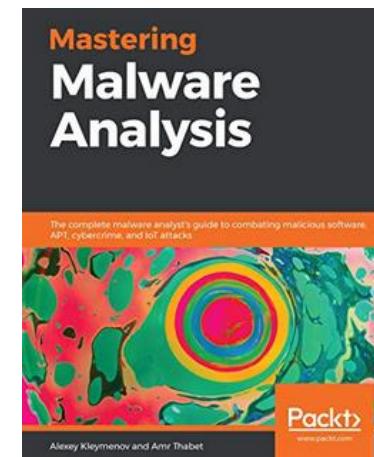
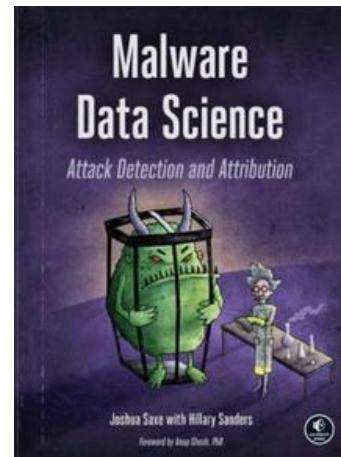
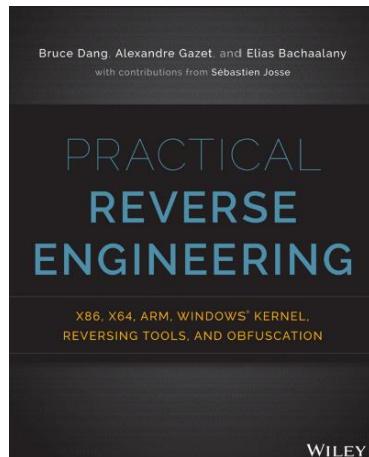
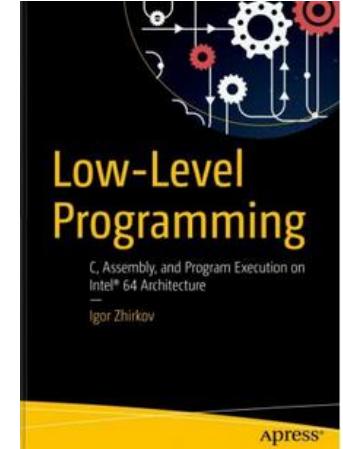
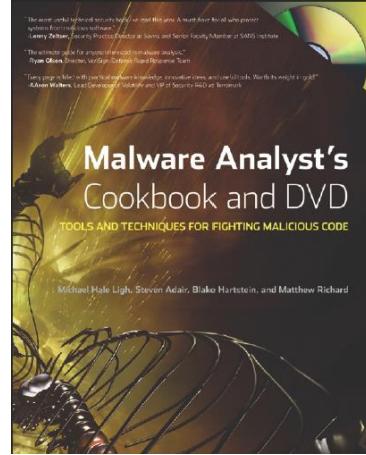
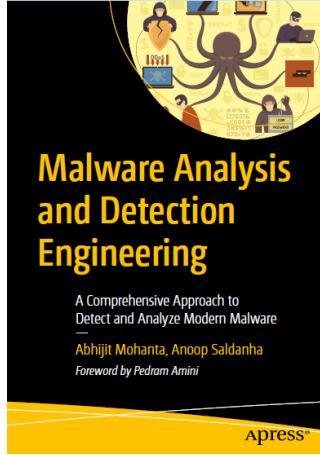
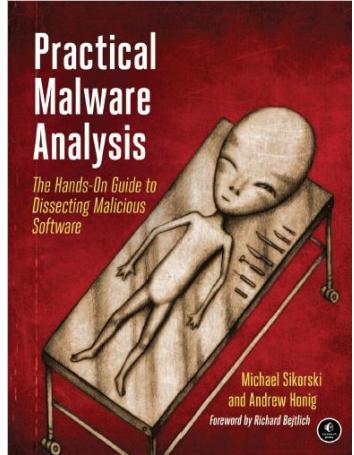
- Caique Barqueta
- Perito Forense, Respondedor de Incidente e Analista de Segurança da Informação... (DFIR) e Analista de Cibersegurança
- Pós-Graduado em Pericia Forense Computacional e Digital
- Pós-Graduando em Segurança Cibernética
- Bacharel em Direito.
- Certificações: ISO27037
- Atuei como Escrivão ad hoc na Policia Civil de São Paulo.



Apresentação do Treinamento

Este curso inicial tem o foco em aplicar a **Análise de Malware voltada para área Forense** mostrando as principais técnicas e ações para prática de análise e identificação de malware, auxiliando assim em perícias ou relatórios que necessitam de elaboração em caso de análise de artefato malicioso.

Referências



Áreas de Atuação

A Análise de Malware poderá auxiliar no aperfeiçoamento em Resposta a Incidentes, Análise em Live, ou seja em caso de SOC, para analistas de cibersegurança, peritos forenses e muitas outras áreas.

Atualmente quem sabe analisar artefatos maliciosos acaba tendo um trunfo nas mangas, pois atualmente todas as empresas e órgão estão sofrendo com ataques de arquivos maliciosos.

Como a Análise de Malware pode me auxiliar?

Análise de Software suspeito

- Funções secundárias maliciosas e busca de comportamentos semelhantes a um trojan
- Entender o funcionamento e descobrir a autoria

Ataques utilizando malware

- Suspeita de ataques a um dispositivo ou infra
- Ambiente comprometido e/ou contaminado
- Busca de vestígios que determinam o objetivo, materialidade e autoria
- Análise *post-mortem*

Malware como elemento secundário

- Malware não tem foco principal
- Funcionalidades semelhantes a spywares
- Obtenção de informações valiosas
 - Senhas para volumes criptografados
 - Registros de conversas instantâneas
 - Dados Bancários

Ética

Uma dica que já deixo é que diariamente para atuação voltada a área forense, é realizada abordagem em ambos mundos, ou seja, tanto para o lado “da luz” quanto para o “sombrio”.

Busque sempre utilizar seu conhecimento para o bem, não utilize para o mal.

E claro, propague qualquer tipo de conhecimento, pois como sabemos, quem compartilha, multiplica.



Introdução aos Conceitos de Análise de Malware

Caique Barqueta



O que é um Malware?

MALICIOUS SOFTWARE ou seja um **Software Malicioso**.

Ele possui a finalidade de se **infiltrar em um sistema computacional**, podendo ser este sistema diverso, como Windows, IOS, Android, Unix...

Ele possui a intenção de **coletar informações sem a autorização** ou de **causar algum tipo de prejuízo a vítima**.

Poderá ser criado de diversos meios, através de **binários, interpretados ou scripts web maliciosos e etc...**

A sua motivação, normalmente vem de obtenção de recursos financeiros, divulgação de informações confidenciais, espionagem industrial/governamental e por ai vai...

Como ocorre a infecção?

Ela poderá ocorrer por vários meios como:

Auto execução de mídias externas onde um dispositivo de armazenamento poderá conter um código malicioso onde ao realizar conectar a dado dispositivo este passa a ser infectado. Normalmente causado pelo Autoruns do Windows e também a auto execução deste script malicioso quando conectado.

Execução consciente do usuário aqui atualmente vemos usuários, como por exemplo aqueles que trabalham em determinada empresa e são recrutados por grupos crackers para prejudicar e causar prejuízos na empresa que trabalha, como por exemplo tornar um sistema indisponível, roubo de informações sigilosas ou acessos privilegiados aos criminosos.

Tipos de malwares:



Spyware:

Ele tem como finalidade a coleta de dados e informações sem o consentimento do usuário, o qual utiliza métodos para obtenção de usuários/senhas de e-mails, números de cartão de crédito, internet banking, busca de carteiras virtuais e acessos a dados armazenados.

Os dados são obtidos por meio de varreduras de navegadores, logins realizados, dados armazenados entre outros...

Existem ainda alguns **subtipos do Spyware**:

- **Adware:** Tem o foco em coleta de informações de consumo e também oferecimento de propagandas.
- **Keylogger:** Tem como o foco realizar a captura das teclas pressionadas pelo usuários.
- **Screenlogger:** Realiza a captura de telas do usuário e até mesmo posição do mouse na tela.



Keylogger



Screenlogger



Adware

Tipos de malwares:

Backdoor:

A backdoor tem a finalidade de ser utilizada após um determinado ataque bem sucedido, que visa **garantir o acesso posterior ao invasor**.

Ela poderá garantir a execução remota de comandos no Sistema Operacional, podendo ser utilizado como proxy.

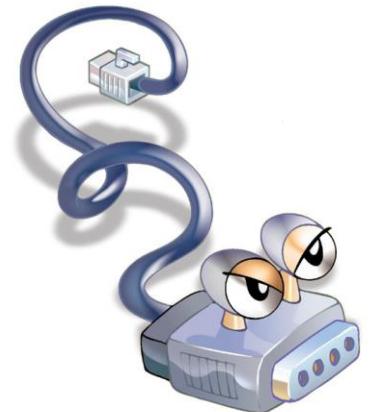
No caso de realização de perícia, poderá auxiliar como álibi em dadas investigações.



Worm:

É um tipo de malware que se propaga por uma rede infectando diversas máquinas distintas por meio de Rede Local ou pela Internet.

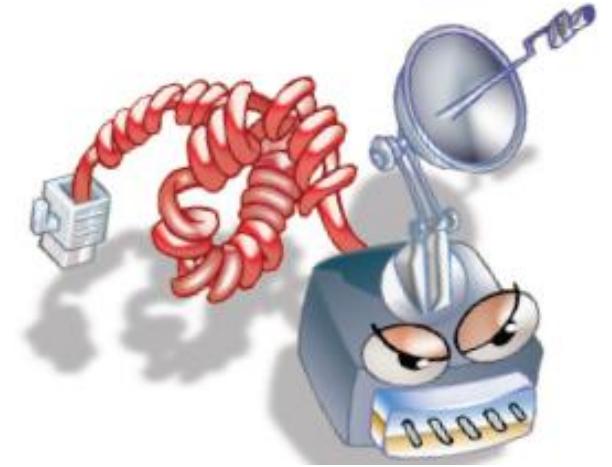
Eles visam **explorar vulnerabilidades** presentes em programas ou serviços de rede e por conta da grande propagação, acaba por **consumir muitos recursos computacionais do ativo**.



Tipos de malwares:

Bot:

Ele pode ser considerado idêntico ao worm em propagação e infecção, porém permite recebimento de comandos externos, garantindo o acesso ao Sistema Operacional violado e acabam recebendo atualizações com novos exploits.

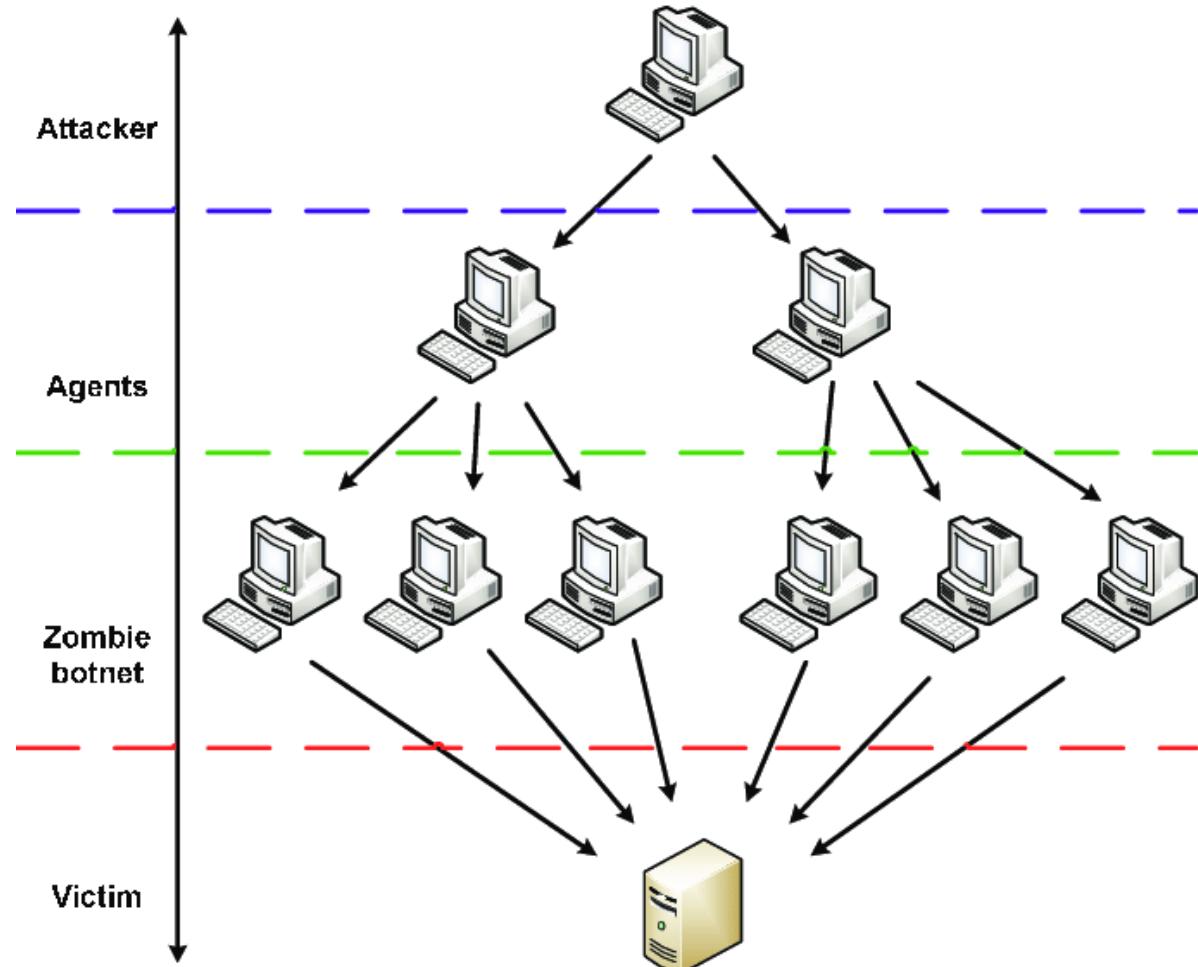


Botnet:

A botnet é uma rede criada por máquinas infectadas por invasores, onde devido a infecção das máquinas, pode ser utilizada para realização de ataques hackers do tipo **DDoS (Distributed Denial of Service)**.



Exemplo de ataque DDoS



Tipos de malwares:

Cavalo de Tróia ou Trojan:

Ele possui funções que aparentam ser inofensivas, porém realiza atividades maliciosas secundárias. O trojan pode ser porta de entrada para outros malwares, como por exemplo:

- Protetores de tela, cursores animados, cracks de softwares, Keygen e etc...



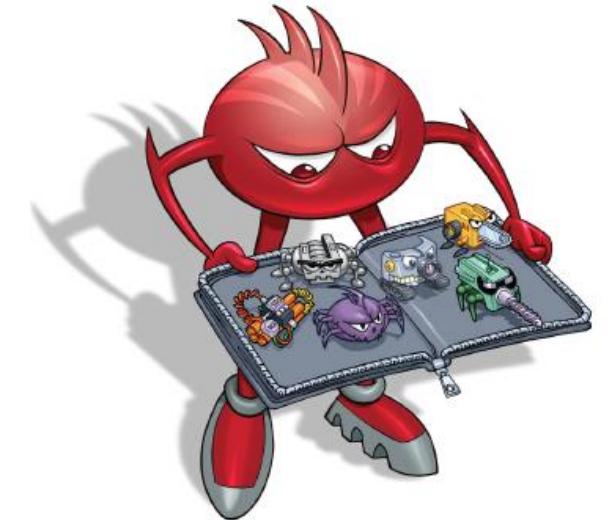
Downloader:

Este tipo de malware foi criado especificamente para realizar o download de outros malwares no ambiente infectado.

Tipos de malwares:

Rootkit:

Este malware tem como finalidade ocultar a presença de um código malicioso, pois podem remover logs do sistema, criptografia de dados, acabam por distribuir seus dados e códigos pelo sistema de arquivos, podem ainda alterar o gerenciador de tarefas e ainda executam em nível de kernel.



Vírus:

Se propaga realizando cópias de si mesmo ou infectando arquivos/programas presentes no computador. Eles necessitam que sejam executados e não fazem o uso de vulnerabilidade em softwares.



Tipos de malwares:

Banker:

Este malware ou trojans foram criado especialmente para realizar a fraude bancária (roubo de acesso de contas, logins e etc...)

Packer:

É um tipo de empacotador de malware, ou seja uma ferramenta usada para mascarar um arquivo malicioso.

Não chega a ser um tipo de malware, mas sim um dos métodos de ofuscação.

Tipos de malwares:

Ransomware:

Este tipo de malware torna os dados armazenados em um equipamento ou sistema inacessíveis, pois geralmente utilizam o método de criptografia e após executarem a referida atividade, realizam a extorsão da vítima para pagamento de resgate dos dados, pagamento este realizado por meio de moedas virtuais, como por exemplo o Bitcoin.

Poderá ainda ser classificado em dois tipos:

- **Locker** que acaba impedindo o acesso ao equipamento, como por exemplo o NotPetya;
- **Crypto** o qual acaba impedindo o acesso aos arquivos armazenados, como exemplo o Wannacry.



Tipos de malwares:

Fileless:

Este tipo de malware foi desenvolvido para não executarem ou escreverem junto ao disco rígido e com isto dificultam a detecção por AV.

Normalmente esse malware utiliza processos legítimos do Sistema Operacional para cometer a atividade maliciosa, como por exemplo o Powershell (PS).

Ele realiza ainda a alteração nos registros do Windows para armazenamento de dados e realizar a auto execução, bem como a execução através da memória RAM (volátil).

Tipos de malwares:

RAT:

Ou mais conhecido como Remote Access Trojan (Trojan de acesso remoto), é um programa que combina as características de um trojan e de backdoor, já que permite ao atacante acessar o equipamento remotamente e executa ações como se fosse o usuário.



Técnicas conhecidas e utilizadas pelos malwares

Alguns tipos de malwares, utilizam técnicas conhecidas (ou não) para realizar a prática de ações maliciosas.

Existe o Mitre ATT&CK e SHIELD frameworks que fornecem referências sobre as técnicas utilizadas:

- <https://attack.mitre.org/>
- <https://shield.mitre.org/>

Mas de cara, posso deixar algumas técnicas de forma mais resumidas:

Compressão: Packers, Encriptação, Metamorfismo, Polimorfismo;

Persistência: Garantia de sobreviver a um reboot (reinicialização)

Escalação de privilégios: Melhorar a permissão de acesso (garantir o admin).

Evasão: Técnicas utilizadas para evitar a detecção por ferramentas de defesa.

Técnicas conhecidas e utilizadas pelos malwares

Roubo de credenciais: Screenloggers, formgrabbers, keyloggers;

Reconhecimento: Aprende sobre a infraestrutura e coleta informações sobre o sistema atacado.

Movimentação lateral: Acesso secundário para atingir objetivo

Execução: Execução de código arbitrário pelo atacante;

Coleta: Coletar informações sensíveis que precede a exfiltração

Exfiltração: Roubo de informações

C², C2 ou C&C: Canal de comunicação entre o atacante e o malware.

Configuração do Ambiente Virtual para Análise de Malware

Caique Barqueta



Configurando um laboratório de Análise de Malware



Lembrando que qualquer tipo de análise de malware requer um ambiente seguro para lidar com o malware, seja realizando a análise estaticamente ou dinamicamente. Necessário tomar determinados cuidados e não executar o malware em sua máquina host e em outras máquinas de produção, infectando-os e, em casos mais graves, infectando outros computadores em sua rede.

A grande maioria dos malware incluem funcionalidades de detecção de ambiente de análise e anti-analise para evitar detecção e análise, também conhecida como uma blindagem. Os sistemas de análise física são mais resilientes às técnicas ante evasão em comparação com os sistemas de análise baseados em Máquinas Virtuais.

Um ambiente para análise física requer ferramentas que criem pontos de restauração do sistema. Algumas das ferramentas que permitem criar pontos de restauração são: Windows System Restore, Clonezilla, Deep Freeze, Time Freeze, Norton Ghost e Reboot Restore RX.

Configurando um laboratório de Análise de Malware



Como alternativa, temos a Máquina Virtual (VM).

O problema de utilizar a VM é que pode ser detectada pelo malware e com isto o mesmo pode não efetivamente causar todo o dano ao ambiente.

Porém as vantagens da VM é que pode realizar Snapshot do ambiente, pois caso ocorra algum problema poderá ser revertido para a imagem que foi realizado o snapshot, ou até mesmo salvar em etapas para que a análise seja completa.

Em seguida, deixo o guia para montar uma Máquina Virtual para realizar a análise de malware em um ambiente virtualizado.

Configurando um laboratório de Análise de Malware



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!

Configurando um laboratório de Análise de Malware



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** em <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”.

Máquina Virtual do Curso



Dúvidas sobre a VM disponibilizada para laboratório e também para o curso.

Deixei outras VM's com sistemas distintos para baixar (Win 10, Win 11 e Win 7), caso queiram utilizar, está no mesmo link.

Vamos utilizar a VM com **Windows 10 64 bits** que poderá ser realizado o download através do link:

https://drive.google.com/file/d/1L_g5quCLEFRfsodU0L2MiaSixWqpUR_S/view?usp=sharing

Usuário: perito

Senha: infected

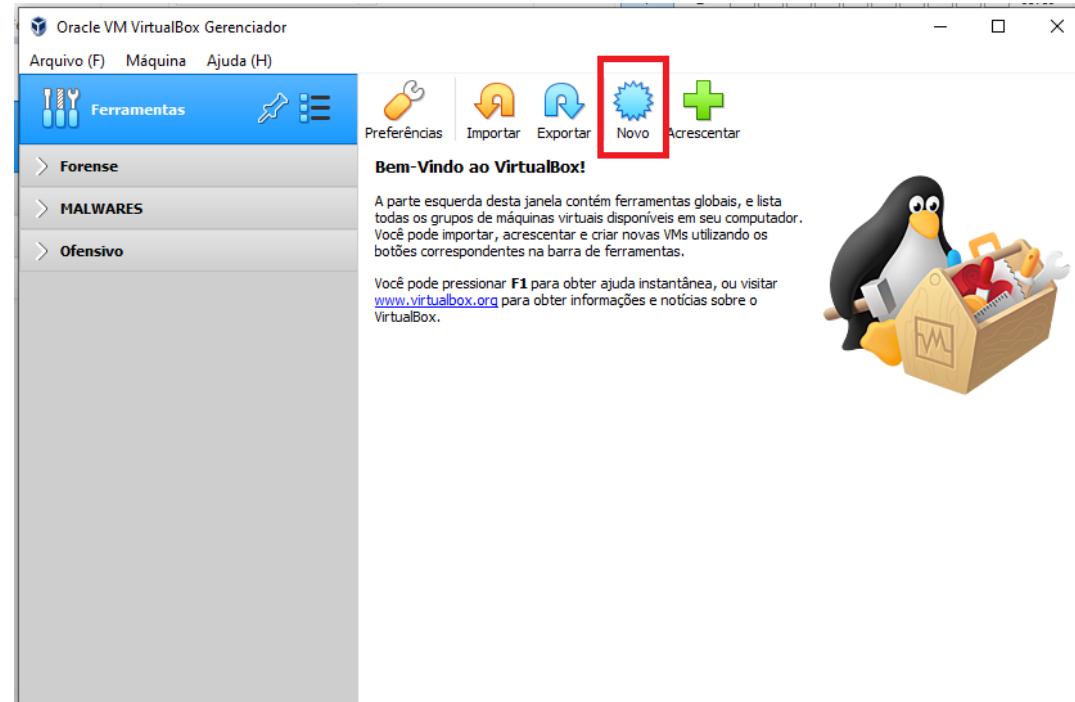
Essa VM está instalada a Flare-VM com todas as ferramentas que vamos utilizar ao longo do curso, bem como contém os arquivos maliciosos que vamos trabalhar para analisar e posteriormente, caso queiram utilizar a referida VM para uso de análise, poderá ser utilizada.

Lembre-se, fez o download e importou a VM, faça Snapshot!

Configurando um laboratório de Análise de Malware

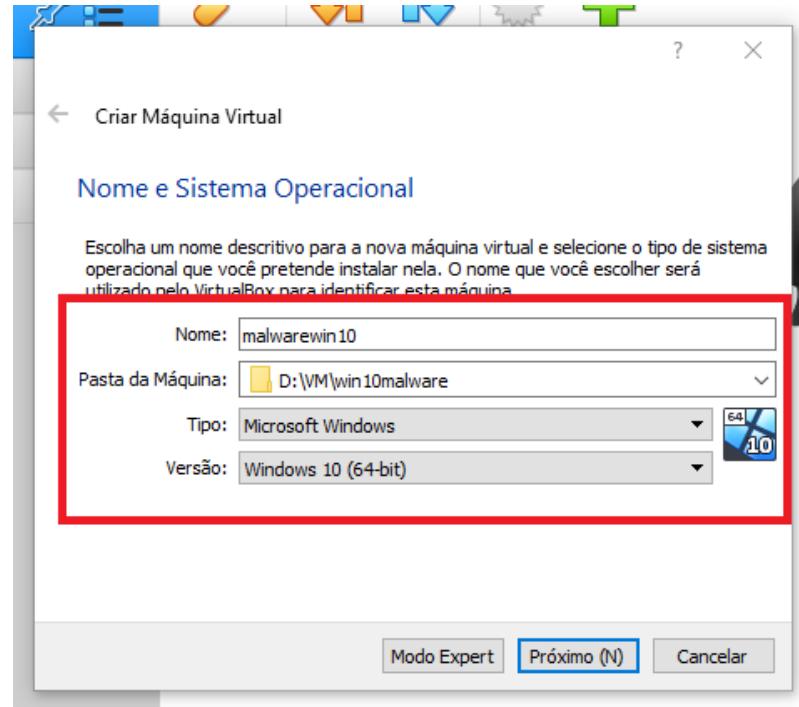


Após baixar e instalar o VirtualBox e sua extensão, clique na opção “Novo”.

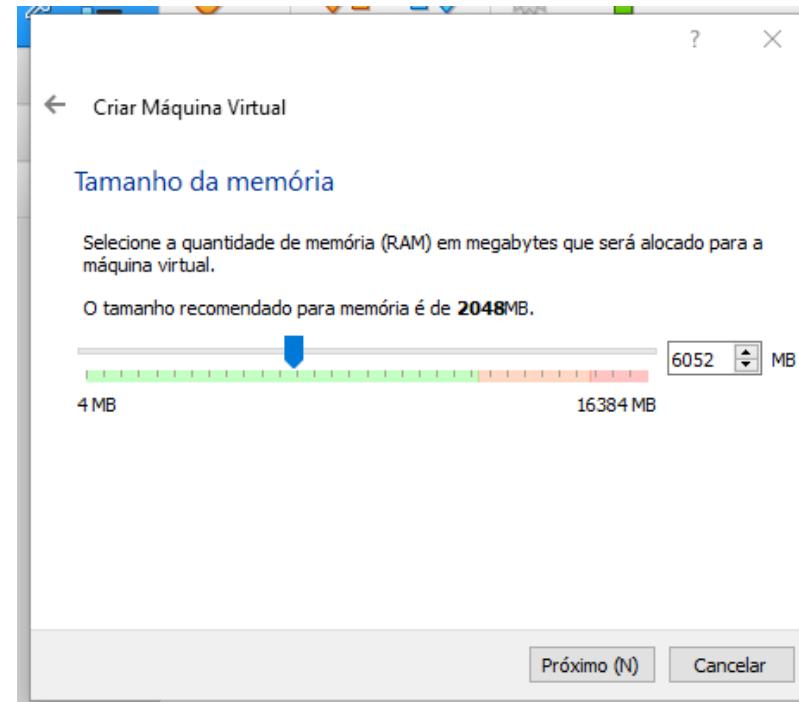


Obs: Percebam que eu já tenho algumas Máquinas Virtuais, caso não tenha, a coluna na esquerda está limpa.

Configurando um laboratório de Análise de Malware



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

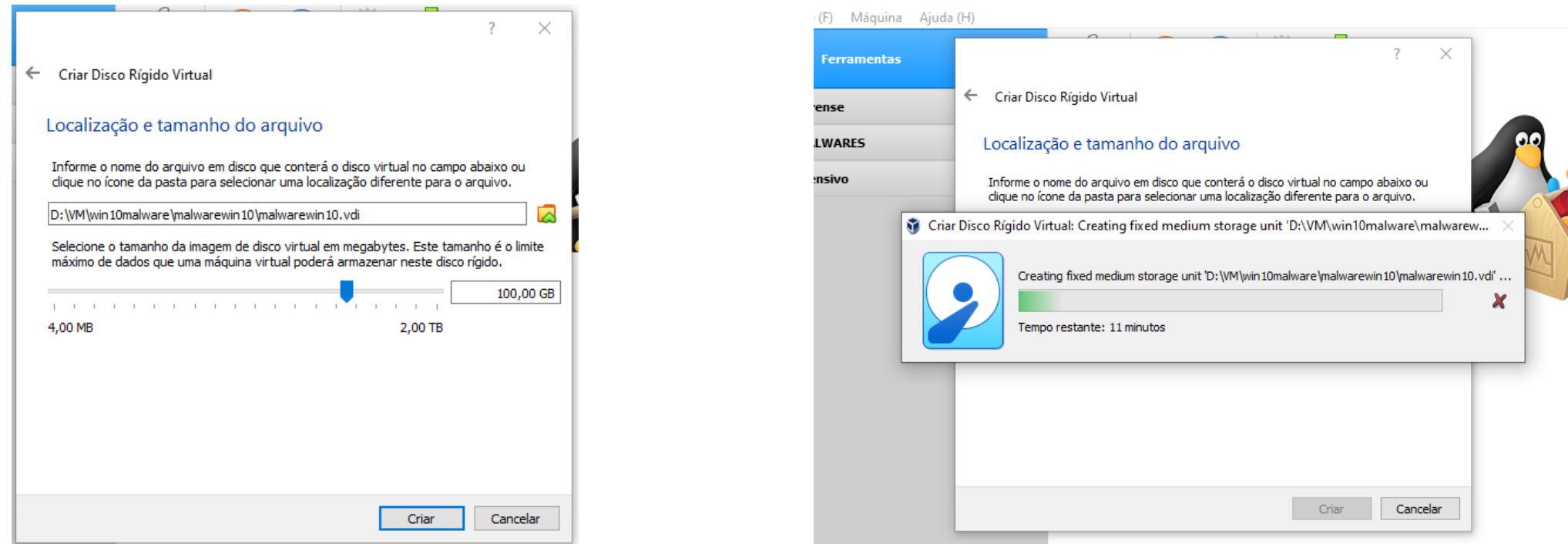


Escolha o tamanho de Memória a ser utilizado pela SandBox.

Configurando um laboratório de Análise de Malware



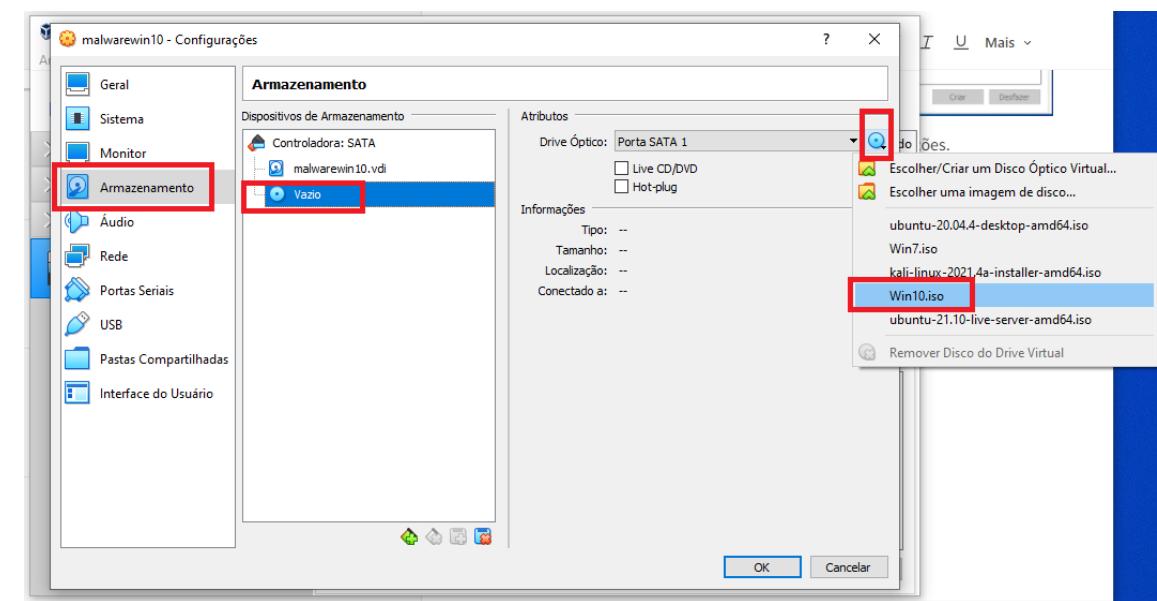
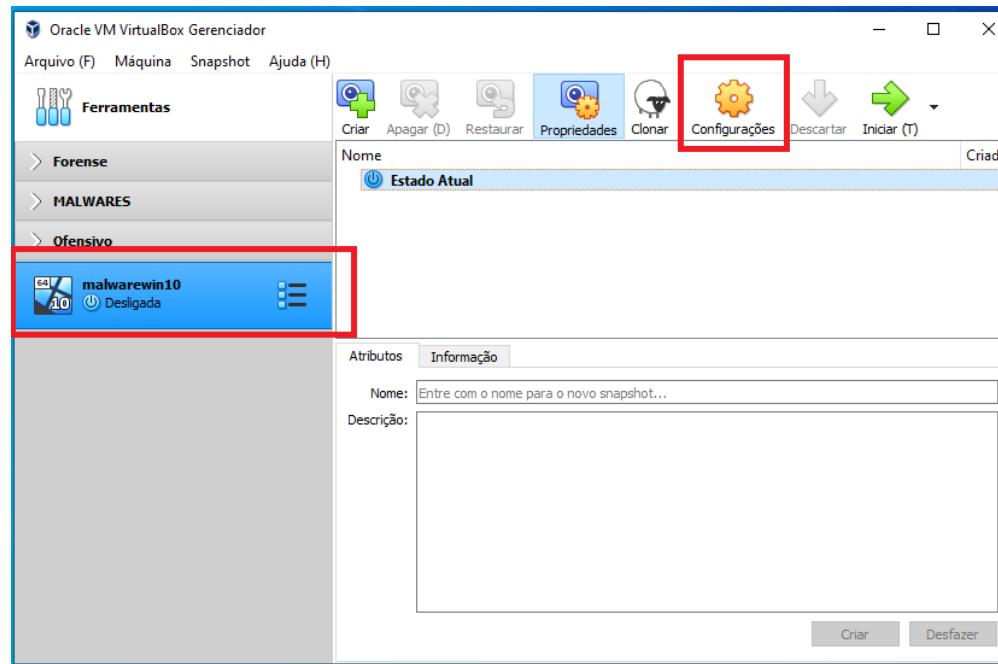
Escolha também o espaço em disco desejado para alocar! Aqui salientei que é bom montar uma com 100GB, você pode montar ela dinamicamente alocada ou fixa, neste caso montei de modo fixo.



Configurando um laboratório de Análise de Malware



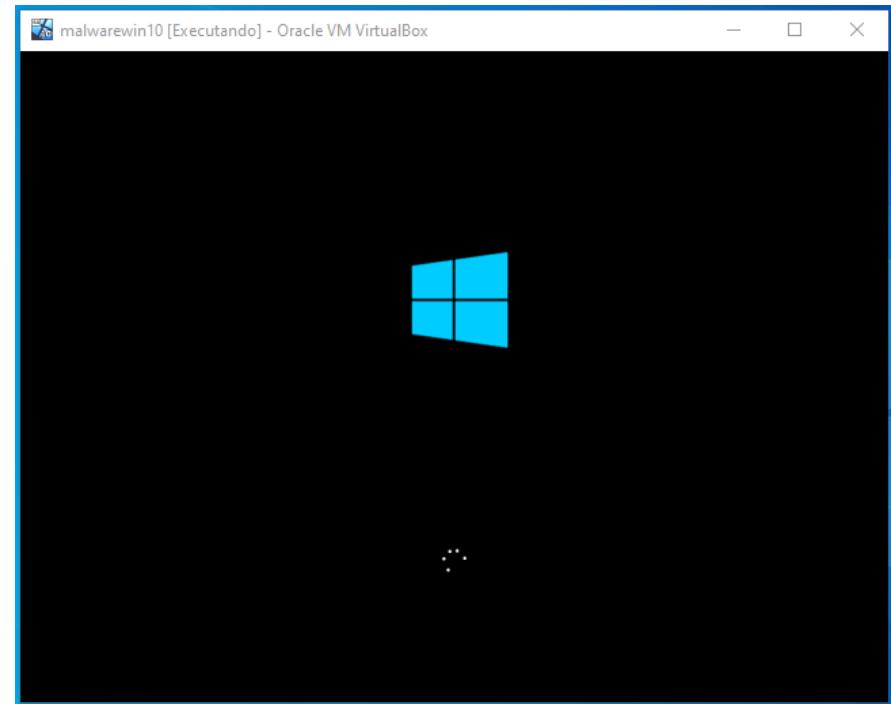
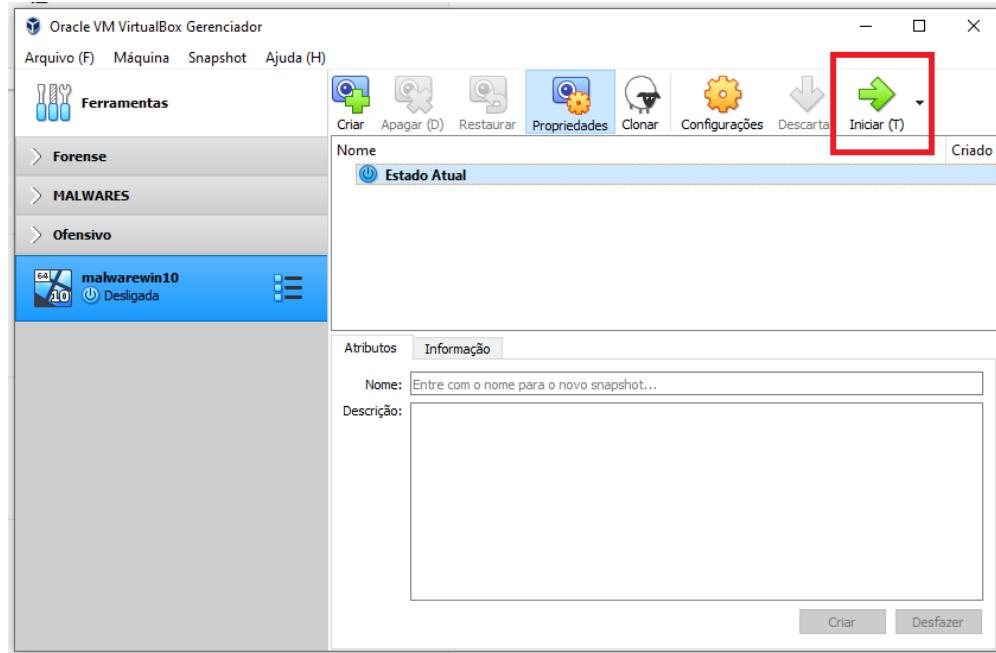
Finalizado a criação da máquina, precisa realizar a utilização da imagem ISO para instalação do Sistema Operacional, para isto selecione a Máquina Virtual criada, vá em Configurações, Armazenamento, na seção de Dispositivos de Armazenamento clique no ícone do CD e em seguida selecione a ISO que utilizará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



Configurando um laboratório de Análise de Malware



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

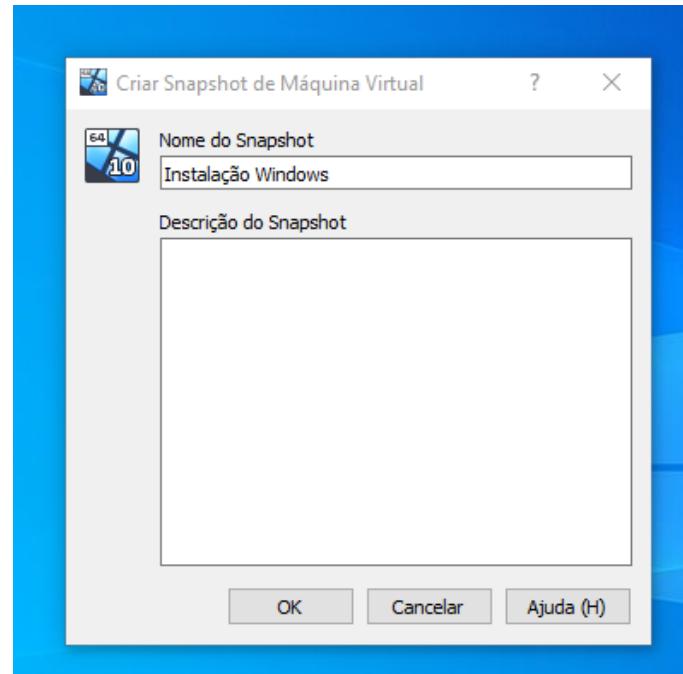


Configurando um laboratório de Análise de Malware



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!



Configurando um laboratório de Análise de Malware



Atualmente, recomendo a instalação do pacote de programas conhecido por **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:

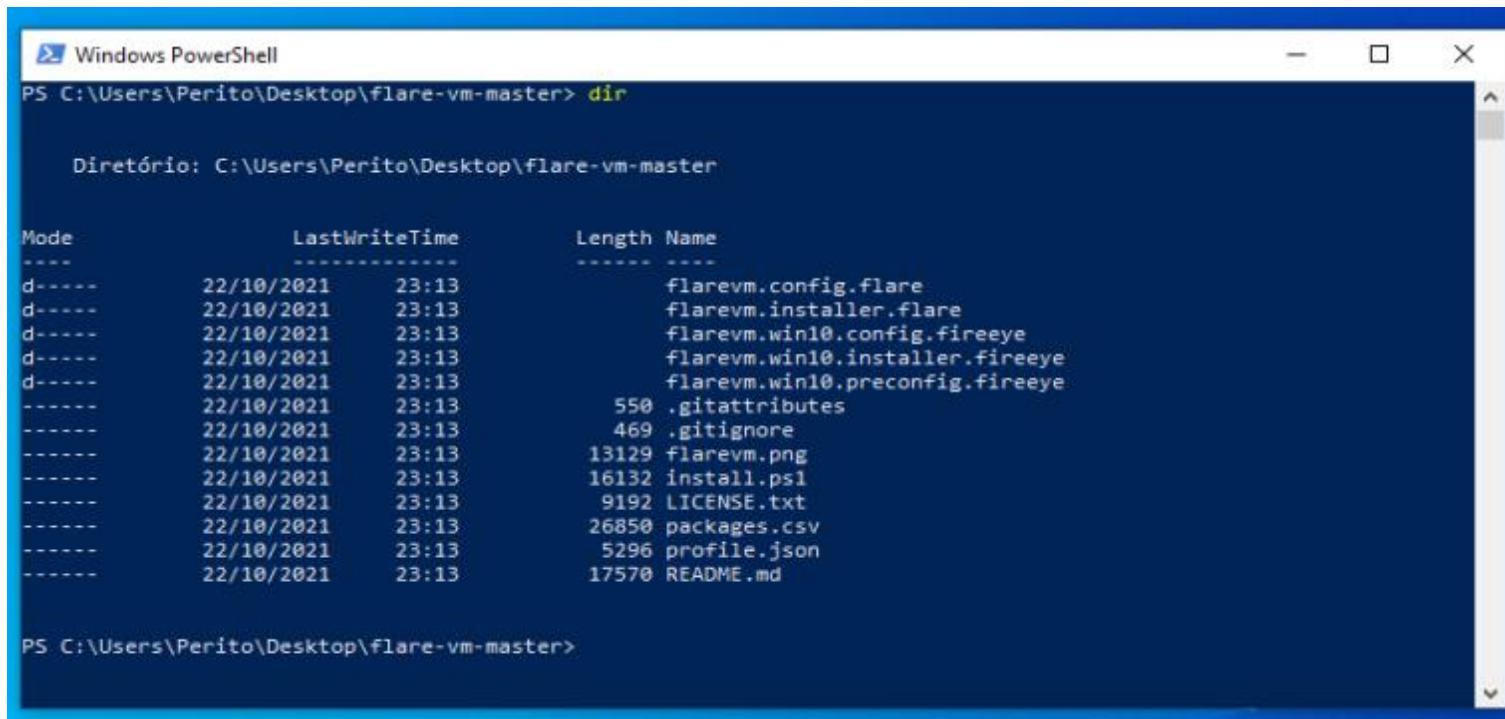
<https://github.com/mandiant/flare-vm>

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

Configurando um laboratório de Análise de Malware



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----
```

Configurando um laboratório de Análise de Malware



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

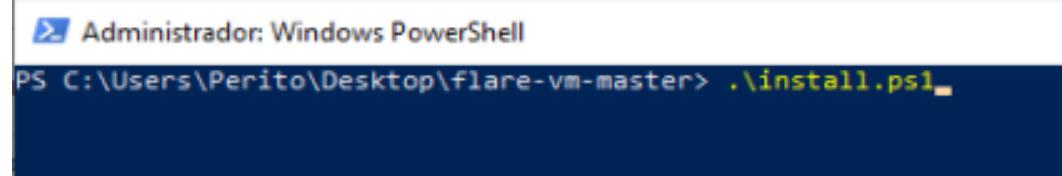
Alteração da Política de Execução
A política de execução ajuda a proteger contra scripts não confiáveis. A alteração da política de execução pode
implicar exposição aos riscos de segurança descritos no tópico da ajuda about_Execution_Policies em
https://go.microsoft.com/fwlink/?LinkID=135170. Deseja 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>
```



Configurando um laboratório de Análise de Malware



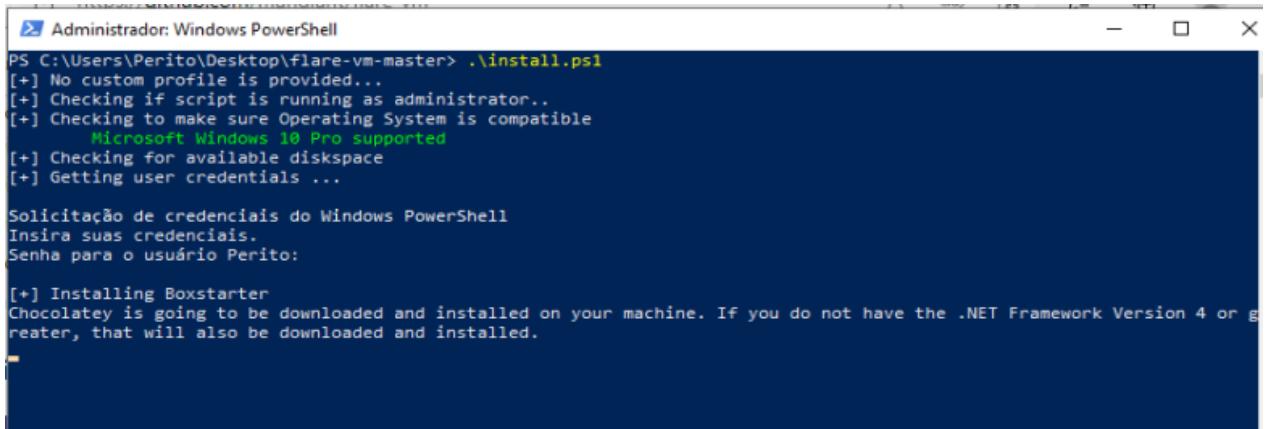
Posteriormente a isto, instale e execute o arquivo .\install.ps1.



```
Administrator: 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.



```
Administrator: 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 diskspace
[+] 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.
```

Ambiente Violado

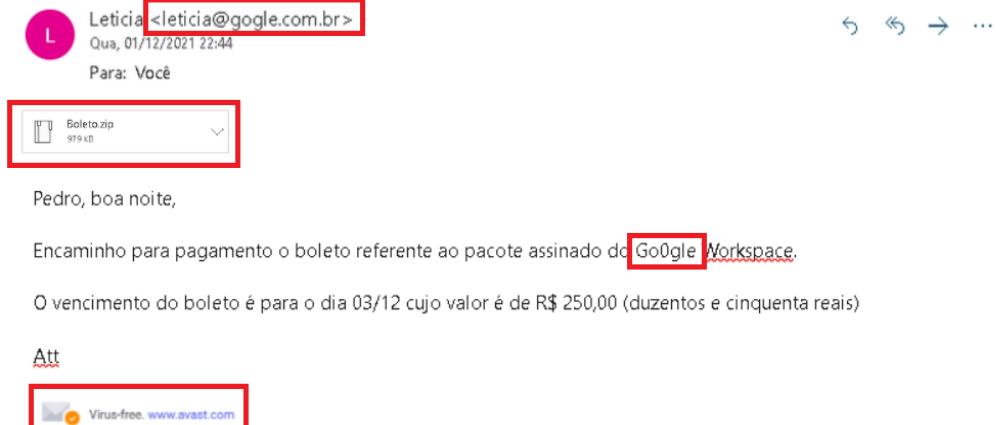
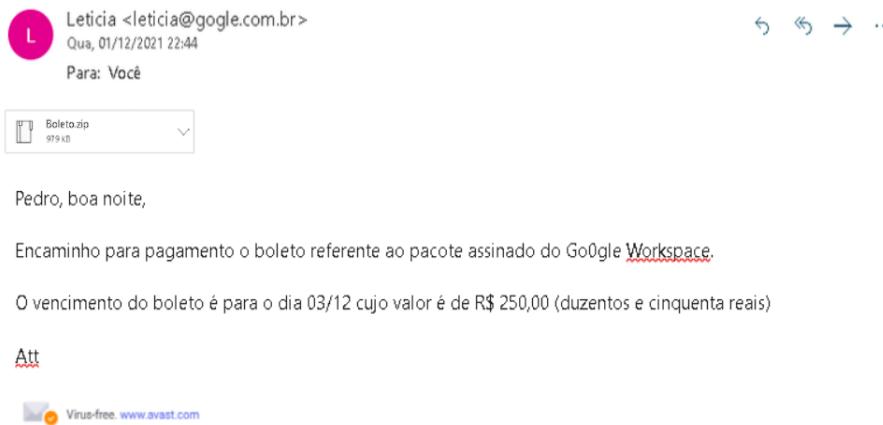
Caique Barqueta



Ambiente Violado

Um dos grandes pontos de que a Análise de Malware poderá nos auxiliar é na questão da identificação do real motivo do arquivo malicioso, ou seja, o que aquele malware realmente faz no ambiente, seja realizando exfiltração dos dados, acesso por meio de backdoor, criptografando arquivos e etc.

Diante disto, imagine que determinado funcionário recebeu e-mail do tipo phishing que continha determinado arquivo malicioso. Inclusive, uma situação na qual a empresa não realiza o acompanhamento de atualizações de sistemas operacionais, não possui antivírus ou algo do tipo, chegando a este colaborador abrindo o arquivo encaminhado/recebido por e-mail.



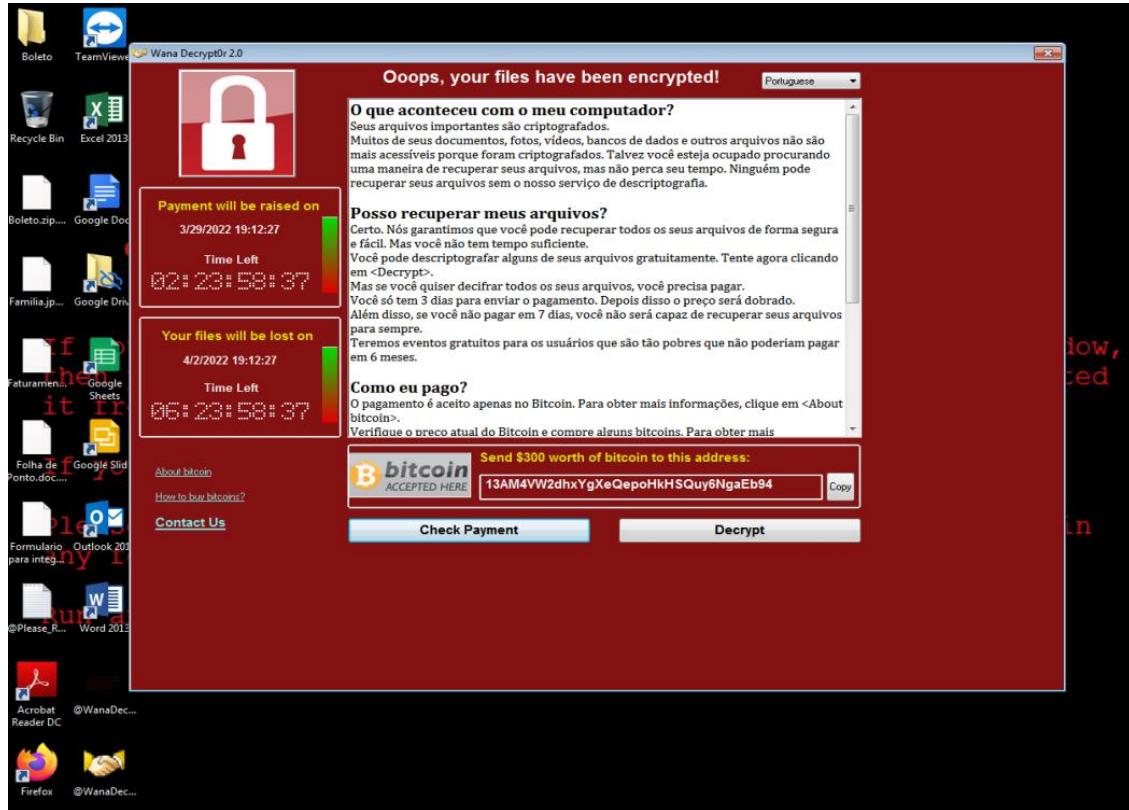
Ambiente Violado

Conforme mencionado anteriormente, colaborador realizou o download de um arquivo compactado com o nome “Boleto”, realizando a descompactação do arquivo e em seguida realizando a execução do mesmo.



Ambiente já está infectado.

A amostra utilizada é a do WannaCry, ou seja um malware do tipo ransomware que realiza a criptografia e por meio de extorsão para liberar o programa para realizar a descriptografia dos arquivos, cuja extorsão se dá por meio de pagamento em Bitcoin para a carteira indicada abaixo.



Ambiente Violado

Após o ataque, a equipe responsável por atender o incidente de segurança conseguiu identificar o arquivo malicioso, realizando a entrega para a equipe realizar a investigação e análise do arquivo malicioso.

Agora, após obter o referido arquivo malicioso que supostamente teria iniciado a criptografia dos arquivos, podemos submetê-lo para diversas análises, as quais iremos abordar em sequência.

Tipos de Análises de Malware

Caique Barqueta



Análise Automatizada



Na análise automatizada, irá apresentar alguns pontos referente a análise do referido malware ou artefato potencialmente malicioso.

Irá apresentar algumas informações relevantes, como tráfego de rede, registro, método de persistência e outros.

Vale lembrar que a análise automatizada não é tão precisa ou minuciosa, sendo que os resultados obtidos devem ser confirmados nas análises estáticas e dinâmica. Inclusive, alguns malwares podem estar programado para somente agir após 5, 10 minutos (exemplo) o que dificulta na análise automatizada.

Cuidado para os documentos que são considerados confidenciais, pois por acabar compartilhando com as referidas ferramentas poderá disponível a toda comunidade.

Outro ponto é que você pode buscar com base no hash do arquivo que está analisando.

Análise Automatizada



- Abaixo algumas opções de sandbox

<https://any.run/>

<https://analyze.intezer.com/>

<https://iris-h.services/pages/dashboard#/pages/dashboard>

<https://capesandbox.com/>

<https://valkyrie.comodo.com/>

<https://www.filescan.io/scan>

<https://intelligence.gatewaywatcher.com/>

<https://tria.ge/>

<https://www.hybrid-analysis.com/>

<https://labs.inquest.net/dfi>

<https://www.joesandbox.com>

<https://malyzer.org/>

<https://sandbox.pikker.ee/>

<https://threatpoint.checkpoint.com/ThreatPortal/emulation>

<https://app.threatconnect.com/>

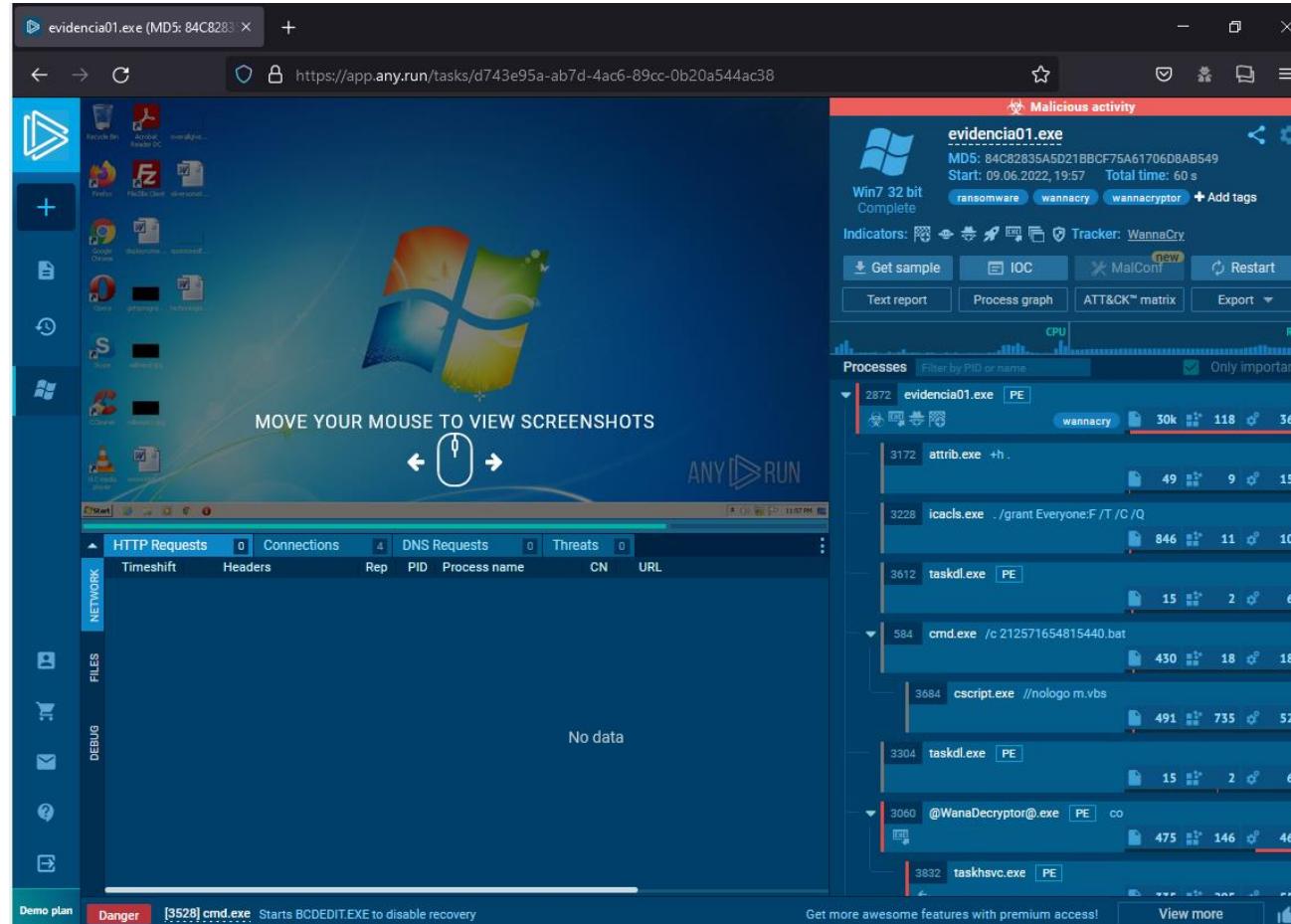
www.threattracksecurity.com/resources/sandbox-malware-analysis.aspx

<https://www.virustotal.com/gui/home/upload>

<https://yomi.yoroi.company/upload>

Análise Automatizada

Exemplo de execução no Any.run o artefato malicioso alvo.



Análise Estática de Malware



Além da automatizada, existem outras duas possibilidades para realizar a análise de códigos maliciosos, sendo:

- **Análise Estática**

É aquela que **não requer a execução do código**, onde você irá obter informações do código/arquivo malicioso sem executá-lo. Nele você poderá **analisar strings, identificar APIs, informações do PE** e irá entender o código de forma descompilada, ou seja o que ele pretende realizar.

Para análise estática você necessitará ter conhecimento em **Assembly** e conhecimento em **Engenharia Reversa** para analisar o código. Além disso, para esta análise mais profunda, é necessário utilizar um **disassembler**, ou seja, um desmontador.

Análise Dinâmica de Malware



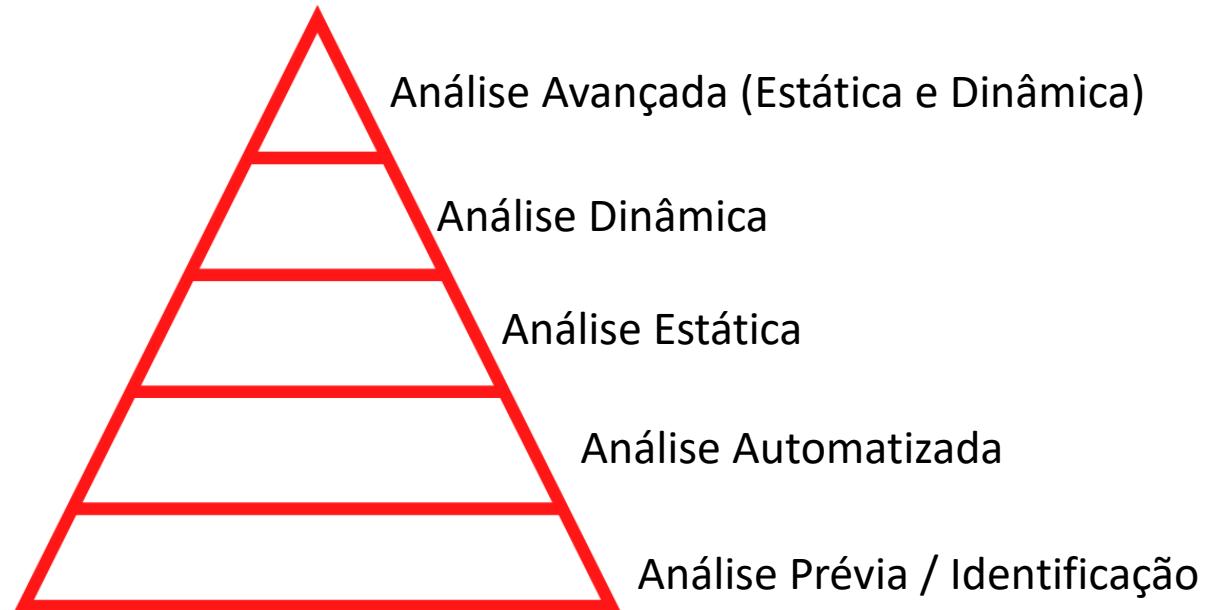
- **Análise Dinâmica**

É aquela que **requer a execução do código**, onde você poderá observar todo o comportamento e alterações que o código/arquivo malicioso realiza no Sistema Operacional. Lembrando que na análise dinâmica você une 2 momentos, **durante a execução e após a execução do código**.

Nele você poderá observar as chamadas que realiza no sistema, alterações de arquivos e registros, conexões externas, havendo também a necessidade de um **debugger** (depurador) e demais informações que forem possíveis identificar.

Existe a possibilidade de utilizar a **análise automatizada**, porém o seu output pode ser limitado.

Cadeia de Análise



Obs. Vale salientar que quanto mais chega na ponta da pirâmide, mais tempo levará a sua análise, porém poderá conter muita informações e detalhes de todo o código malicioso, visto que será realizado uma análise mais completa possível.

Principais pontos a serem verificados e respondidos

Caique Barqueta



Perguntas a serem respondidas

- O arquivo questionado é considerado potencialmente malicioso por algum antivírus? Quais informações poderão ser obtidas?
- Há indicação de qual compilador utilizado? Quando o arquivo foi compilado?
- Há indicação de que esse arquivo questionado está compactado ou ofuscado? Se sim qual é o indicador?
- Este arquivo malicioso realiza alguma importação? Se sim, qual(is) ele faz?
- Existem outros arquivos ou indicados baseados em host que você poderia procurar em sistemas infectados?
- Quais indicadores baseados em rede podem ser usados para encontrar esse malware em máquinas infectadas?
- Entre outras perguntas relevantes...

Análise Estática

Como demonstrei ao vivo, segue algumas etapas e ferramentas para serem utilizadas em caso de análise estática.

- Acesso ao **VirusTotal** (<https://virustotal.com.br>) para realizar a consulta do referido executável. (Aqui é possível já identificar e ter certeza do tipo de malware).
- Abertura do arquivo no **Pestudio (versão 9.30)** para que possamos realizar a análise posteriormente, visto que demora um pouco para o programa abrir ou ser totalmente carregado.
- Abertura do arquivo malicioso no **Detect It Easy (versão 3.01)** para que possamos identificar Strings, Importações, dados do compilador utilizado, verificar se existe algum *Packer* (arquivo escondido), data de compilação e demais informações relevantes. Caso queira poderá utilizar o **Exeinfo (versão 0.0.5.3)** também para análise.

Análise Dinâmica

A seguir, vamos preparar o ambiente para execução do referido arquivo malicioso.

- Abrir o **Autoruns** e fazer o backup dos registros e serviços utilizados na inicialização do arquivo.
- Abrir o **Procmon** para monitorar os processos criados, arquivos escritos e demais informações relevantes na execução do malware.
- Abrir o **FakeNet** para capturar as requisições de rede que o malware realizar.
- Abrir o **RegShot** e realizar o 1 “shot do sistema” e após a execução, realizar o 2 “shot”.
- Abrir o **FileGrab** para capturar os arquivos criados pelo malware
- Abrir o **ProcessHacker** para monitorar o processo do referido malware.

E dai em diante é realizar a análise dos artefatos interessantes para a perícia.

Análise Estática e Dinâmica Avançadas

Poderá ocorrer ainda a necessidade de realizar a Análise tanto Estática quanto Dinâmica de modo mais avançado ao arquivo questionado quando não há identificação de todas as informações necessárias. Neste caso você irá explorar e analisar o código mais profundamente e também analisar funcionalidades específicas contidas no executável.

Requer um conhecimento em Assembly, bem como há necessidade de **disassembler** para que seja analisado as strings e imports do arquivo PE e também de **debuggers** para analisar a execução do referido arquivo.

Nestas análises você irá observar as informações utilizadas pelo arquivo em memória principal (RAM) e também no disco.

Exemplos de programas utilizados para análise mais avançada:

- **IDA Pro (disassembler)**
- **OllyDbg**
- **X64dbg ou x32dbg**
- **WinDBG**

Muito obrigado!

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

Telegram: [@caiquebarqueta](https://t.me/caiquebarqueta)

Arquivo sobre como montar sua Sandbox para análise de malware

https://drive.google.com/file/d/1oXPJ_eVKlttgXfHJGdBgNApvce5vNBAG/view?usp=sharing



AFD
Academia de Forense Digital

📞 (11) 9 8594-6809

✉️ @academiadeforensedigital

🌐 www.academiadeforensedigital.com.br