Análise a software malicioso: técnicas e ferramentas

Catarina Silva, *Estudante, ESTG* Gonçalo Vicente, *Estudante, ESTG*

***Resumo*—Nos dias de hoje, a existência de *software* malicioso está cada vez mais entranhado no mundo da informática. Neste sentido existe a necessidade de estar atento e saber que técnicas, que tipos de análise e ferramentas podem ser utilizadas de forma a combater estes *softwares* nocivos e de consciencializar a população para os perigos que, hoje em dia, percorrem a internet.**

Neste trabalho, será analisado, com recurso a um caso prático, o comportamento de um *software* malicioso em particular, denominado de *WannaCry*, colocando assim em prática uma das ferramentas mais conhecidas para a realização de análise estática, o Yara. O *setup* utilizado envolve a infeção propositada de uma máquina virtual para o efeito. Para isso, executaram-se as regras Yara através de opções de comandos específicas, de modo a obter um *output* que fosse compatível com as *strings* propostas pelas regras que foram utilizadas na análise dos ficheiros recolhidos da máquina infetada.

Com base no output obtido pela execução das regras sob o diretório onde se encontrava a pasta com os ficheiros infetados, conseguiram-se reunir um conjunto de strings que permitiram identificar as várias assinaturas correspondentes ao *sofware* malicioso *WannaCry*.

***Palavras-chave*—Malware, Ransomware, Strings, WannaCry, Yara.**

I. Introdução

De modo a combater o crescimento do Cibercrime, surgiu o conceito e a prática de Cibersegurança, que consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no Ciberespaço, e das pessoas que nele interagem. [1]

Dos maiores objetivos que a Cibersegurança visa alcançar, é a luta diária contra softwares maliciosos. *Malware* é um software malicioso ou intrusivo que visa danificar e destruir os computadores e os sistemas operativos, de modo a adquirir informação seja esta, maioritariamente, em prol de obtenção de lucro, mas também poderá ser utilizado para obtenção de propriedade intelectual. [2]

Um dos tentáculos do *Malware*, quiçá o mais utilizado, é o *Ransomware*. O *Ransomware*, impede ou limita o acesso dos utilizadores ao seu sistema ou aos seus dispositivos, exigindo-lhes o pagamento de um resgate através de certos métodos de pagamento em linha (e dentro de um prazo estabelecido), a fim de recuperarem o controlo dos seus dados.

O presente trabalho foi realizado em contexto universitário, no âmbito da unidade curricular de Administração Segura de Sistemas Informáticos, do Mestrado em Cibersegurança e Informática Forense que aborda as técnicas e as ferramentas que se poderão utilizar aquando a análise de *software* malicioso.

Ao longo deste documento serão abordados conceitos como o que é *Malware*, de que forma é que este é propagado e planeado, os vários tipos de *software* malicioso que existem e as suas particularidades, as várias maneiras que se poderá proceder para fazer a sua análise e por fim um contexto prático, a título de exemplo, de modo a colocar em teste uma das ferramentas mais conhecidas, mais utilizadas para este tipo de casos e mais abordada em contexto académico.

II. Malware

Malware, como o próprio nome indica, é um *software* malicioso ou intrusivo que visa danificar e destruir os computadores e os sistemas operativos, de modo a adquirir informação seja esta, maioritariamente, para fazer dinheiro, mas também poderá ser utilizado para obtenção de propriedade intelectual.

Quando se pretende obter propriedade intelectual, utilizam-se os APT's (*Advanced Persistent Threat*) que consistem num ataque prolongado com enfoque num alvo específico, tendo como objetivo comprometer um sistema e exfiltrar informações sobre esse mesmo alvo. Por exemplo, o *Ghostnet* utilizado pela China e o *Skyipot APT* colocado em ATM's (caixas de multibanco).

Estes ciberataques estão, alegadamente, ligados a cibercriminosos ou grupos patrocinados pelo Estado, mas também podem ser executados por grupos individuais para atingir os objetivos que delinearam para a execução de determinado ataque.

III. Modus Operandi

Antes de qualquer criação deste tipo de *software* é necessário que exista um estudo prévio do alvo escolhido, de modo a encontrar as vulnerabilidades através das quais o possam atingir.

Escolhido o alvo e identificadas as suas vulnerabilidades, o *Malware* é propagado por portos abertos, por exemplo, o porto 80 que é responsável pelos pedidos http (navegação na internet). No caso de este porto se encontrar fechado, seria impossível conseguirmos navegar na internet.

Através deste acesso, para que o *Malware* não desapareça mal se feche a página de navegação que o alvo tinha aberto, este propaga-se de *browser* em *browser*, isto é, podemos estar no *Internet Explorer* e se abrirmos o *Google Chrome* este migra automaticamente para a segunda página que se abriu.

Por outro lado, também existe *Malware* que se aloja de imediato no *Registry*, utilizando as funcionalidades do sistema operativo contra o próprio utilizador. Isto dificulta a sua deteção, já que o código malicioso é executado através de processos legítimos.

Uma das principais características para que a utilização deste tipo de *software* seja proveitosa, consiste na persistência que o *Malware* necessita de ter, persistência esta que é adquirida através da passagem de processo a processo.

IV. Formas mais comuns de infeção por software malicioso

Os cibercriminosos utilizarão técnicas de engenharia social e técnicas de *phishing* para atrair os seus alvos, de modo a obterem propriedade intelectual ou monetária, recorrendo, assim, às seguintes formas [2]:

A. Através de emails

Poderá acontecer com a abertura de anexos suspeitos ou não solicitados no corpo do email ou através de links que se encontrem presentes em *emails* de *spam* ou que apresentem indícios de *phishing*.

B. Através de Websites

Clicando em links que redirecionam para páginas web desconhecidas ou apenas visitando websites específicos, como por exemplo, websites destinados a conteúdo sensível para adultos.

C. Através de Janelas de Pop-ups

Clicando nesses mesmos pop-ups para fazer downloads de *software* ou em anúncios que aparecem em websites a aliciar as pessoas a clicarem naqueles pop-ups, maioritariamente, de publicidade.

D. Através de Redes Wi-Fi abertas

Os atacantes utilizam este tipo de redes para recolher informações consideradas propriedade intelectual ou para tentarem obter o controlo total dos sistemas eletrónicos do alvo escolhido.

E. Através de Software

Descarregando software pirateado ou gratuito, como por exemplo, jogos ou descarregar ficheiros através de redes *peer-to-peer*.

F. Através de dispositivos USB

Colocando software malicioso num determinado dispositivo USB e conectá-lo a um dispositivo eletrónico do alvo que se pretende atingir, de modo a comprometer os sistemas e, por sua vez, a informação que consta nos mesmos.

V. Tipos de Malware

A. Trojan

1) O que é?: Consiste, à primeira vista, num software legítimo ou incorporado num que apresente utilidade para quem o quer utilizar, mas acaba por se revelar num programa delineado para intenções maliciosas.

2) O que é que faz?: O propósito para o qual foi criado depende da motivação do atacante, isto é, tanto pode ser utilizado para espionagem, roubo de dados, eliminação de ficheiros, para expandir uma *botnet* ou para executar ataques *DDoS*.

3) Como é que se espalha?: Requer algum tipo de interação proveniente de um utilizador, seja através da abertura de um anexo recebido por email ou pelo download/execução de um ficheiro a partir de um *website*. Para que estas opções tenham uma maior taxa de sucesso, os atacantes recorrem a metodologias como a engenharia social.

B. Ransomware

1) O que é?: Visa evitar ou limitar os utilizadores ao acesso dos seus sistemas, dispositivos ou informação, sendo exigido o pagamento de um resgate de uma determinada forma, escolhida pelo atacante e dentro de um determinado espaço temporal, a fim das vítimas deste tipo de ataques reaverem o controlo das informações ou sistemas que foram comprometidos.

2) Tipos mais conhecidos de Ransomware:

a) *Winlocker*: Bloqueia o ecrã do dispositivo e restringe o acesso a todo o sistema.
Um dos *Winlockers* mais conhecidos é o *Police Ransomware* que basicamente utiliza simbologia característica a assuntos relacionados com a lei para garantir autoridade no contacto estabelecido, de modo a coagir as vítimas a fazer o pagamento para reaverem as suas informações.
Normalmente, a abordagem que utilizam para com os seus alvos é feita através de um email relativo a processos como: Atividades ilícitas realizadas no ciberespaço, partilha de arquivos confidenciais ou acusações de posse de conteúdo infantil.

b) *BitLocker*: Encripta ficheiros relevantes, como registos fotográficos, documentos ou informações retidas em base de dados e as bases de dados propriamente ditas.

3) Como é que se espalha?: Pode ser descarregado por meio de atualizações falsas de aplicações ou através da visita de *websites* comprometidos. Também pode encontrar-se camuflado em anexos enviados por email, *emails* esses considerados *spam* ou não solicitados, com recurso a outro *malware*, por exemplo um *Trojan*. Normalmente, neste tipo de ataques, o aconselhável é nunca pagar o resgate, visto que não existe garantia nenhuma de voltar a reaver o acesso aos ficheiros e informações comprometidas.

C. Backdoor

1) O que é?: Corresponde a uma aplicação que permite realizar acesso remoto e não autorizado a um sistema ou à máquina que se pretende atacar.

2) O que é que faz?: Fornece, ao atacante, o acesso quase total da máquina, permitindo ao mesmo realizar um conjunto amplo de ações, sendo estas: monitorizar, interceptar, modificar e interferir na máquina em questão.

3) Como é que se espalha?: Este tipo de *software* pode ser detetado, se efectivamente existir, ou instalado através da utilização de outro tipo de *malware*. Os RAT's (*Remote Administration Trojans*), tanto são *Trojans* como *Backdoor*, ou seja, ambos são aplicações que concedem a permissão de controlo de acesso remoto.

D. Spyware

1) O que é?: É uma aplicação que é instalada, involuntariamente, num computador ou num dispositivo informático, para monitorizar a atividade dos utilizadores e transmitir as informações ao atacante responsável pela mesma.

2) O que é que faz?: Rastreia a atividade dos utilizadores na Internet e recolhe informações sem o conhecimento do mesmo, informações essas: *websites* visitados, dados pessoais referentes ao utilizador do sistema, senhas etc. Este tipo de *software* como consome uma quantidade considerável de memória do dispositivo, vai fazer com que este fique mais lento.

3) Como é que se espalha?: O *Spyware* pode interceptar os dispositivos de várias formas, através de outro tipo de *malware* ou através da visita de *websites* que no seu conteúdo possuem *softwares* maliciosos.

E. Adware

1) O que é?: Software malicioso que exibe *banners* publicitários ou janelas *pop-up* enquanto um programa está em execução.

2) O que é que faz?: Na sua arquitetura, inclui código que permite fazer o rastreio do comportamento de utilizadores na Internet e reúne informações sem o consentimento do utilizador, maioritariamente, para fins publicitários.

3) Como é que se espalha?: Encontra-se, geralmente, integrado em *downloads* de programas gratuitos ou de baixo custo.

F. Scareware

1) O que é?: Aplicação que simula *scans* para encontrar vestígios de algum tipo de *malware* no dispositivo do alvo em questão, quando na verdade o *scan* é feito à informação disponível do equipamento, levando a vítima a pagar pela suposta remoção.

2) O que é que faz?: Estabelece um valor padrão que ronda entre os 50 e os 100 euros, pela dita remoção do *malware* e se o utilizador pagar essa quantia pelo serviço prestado, os dados referentes ao seu cartão multibanco ou de crédito podem ser roubados.

3) Como é que se espalha?: Utilizam várias técnicas para convencerem os seus alvos, como seja: emails de spam, mensagens com ficheiros multimédia que ao clicar nas mesmas, desencadeiam a execução de *software* malicioso ou *websites* comprometidos com avisos sobre segurança falsos.

G. Worm

1) O que é?: Malware que se replica ao longo de uma rede de computadores, executando assim, ações tendencialmente maliciosas, explorando, automaticamente, as vulnerabilidades que deteta sem orientação manual adicional.

2) O que é que faz?: Podem causar danos devido ao excessivo consumo de memória do dispositivo onde se encontram alojados e com excluir arquivos ou enviar documentos indesejados por email.
Para além disso, podem ser utilizados como intermediário para a instalação de outros tipos de *software* malicioso, como *backdoors*. São ainda utilizados para ampliar redes de *botnet*.

3) Como é que se espalha?: Não necessitam de intervenção manual para se proliferar, visto que o fazem através de uma rede, via email, partilha de arquivos troca de dispositivos USB e executar links redirecionados para *websites* maliciosos.

H. File Infector Virus

1) O que é?: Tipo de *malware* que infeta executáveis, substituindo-os ou injetando nos mesmos código malicioso, com o intuito de causar danos permanentes nos dispositivos que correrem aqueles ficheiros ou tornar os mesmos inutilizáveis.

2) O que é que faz?: Provoca pequenas perturbações ou, em casos mais avançados, danos no próprio equipamento em que se encontram alojados, tendo como desfecho a formatação total do dispositivo.

3) Como é que se espalha?: Por auto-replicação e anexando-se a ficheiros executáveis. Assim, sempre que se correr o executável, o software malicioso será, igualmente, executado.

I. RootKits

1) O que é?: É uma aplicação que permite o acesso aos privilégios de administrador de um dispositivo ou de uma rede de equipamentos. Uma vez instalado, este mascara o facto de que o sistema foi comprometido, permitindo que o atacante obtenha acesso remoto ou privilegiado ao dispositivo e, possivelmente, a outras máquinas que se encontrem na mesma rede.

2) O que é que faz?: Pode ser utilizado para casos de *spyware*, monitorização de tráfego, alteração de log's, para atacar outras máquinas na rede e para alterar ferramentas do sistema responsáveis pela deteção deste tipo de *softwares*.

3) Como é que se espalha?: Requer interação do utilizador para que seja instalado no sistema.
Se um *rootkit* for detetado, talvez seja necessário formatar o disco rígido do computador e reinstalar o sistema operativo.

VI. Análise de Malware

Para se entender melhor o funcionamento, as características do *malware* e avaliar o impacto do mesmo sobre um sistema, devemos sempre tentar usar diferentes técnicas de análise. No que concerne à análise propriamente dita do *Malware*, esta pode ser: Estática, Dinâmico ou comportamental, análise do código e por fim, análise de memória.

A. Análise Estática

Consiste em analisar a *sample* (cópia binária) sem a executar, com o intuito de extrair metadados sobre o *malware*. Esta pode não revelar todas as informações necessárias, mas às vezes pode fornecer informações interessantes que ajudam a determinar onde concentrar os esforços de análise subsequentes.

As ferramentas mais utilizadas para a realização deste tipo de análise são:

a) o Yara, que será abordado com mais pormenor na parte prática que se decidiu realizar;
b) o FuzzyHashing, que é uma função de compressão para calcular a similaridade entre arquivos digitais, sendo útil para tentar automatizar o processo de agrupamento de *malware* semelhante, podendo fornecer informações do quão diferentes são dois arquivos, comparando apenas a semelhança dos seus *outputs*.
   Essa propriedade é útil para fazer a análise de, por exemplo, *clustering malware campaigns*, visto que estas utilizam, geralmente, inúmeras variantes da mesma família de *software* malicioso que executam exatamente o mesmo conjunto de comportamentos, mas acabam por apresentar *hashes* criptográficos diferentes. [3]

B. Análise Dinâmico ou Comportamental

Nesta tipologia de análise, é essencial a execução do binário, em ambiente "selado", ou com recurso a uma máquina virtual, reportando sempre ao EMAS. O EMAS (*Europol Malware Analysis Solution*) é uma plataforma de análise de *malware* restrita à aplicação da lei, propriedade e alojada pela *Europol*, que suporta a análise forense do comportamento de *malware* e concentra-se no enriquecimento de investigações transfronteiriças relacionadas com *malware*.

Para a execução desta análise podemos utilizar ferramentas como o *Wireshark* e o *Process Monitor*.

O *Wireshark* é um programa que analisa o tráfego de rede e organiza-o por protocolos. Esta ferramenta apresenta funcionalidades idênticas ao *tcpdump*, porém apresenta uma interface gráfica com mais informação e com a possibilidade de recorrer a filtros para uma melhor experiência de utilização. [4]

O *Process Monitor* é uma ferramenta de monitorização para Windows que mostra o sistema de ficheiros em tempo real, o registo e as atividades dos processos. Esta ferramenta tem como recurso duas outras ferramentas da *Sysinternals*: a *Filemonitor* e a *Regmonitor*. [5]

C. Análise de código

Consiste numa técnica mais avançada que as suprarreferidas, pois permite validar e entender o funcionamento interno do binário do *malware*.
A análise de código pode dividir-se em duas vertentes: Na análise de código estático e na análise de código dinâmico.

a) Análise de código estático: A análise de código estático envolve "desmontar" o binário suspeito e examinar o código para entender o comportamento do programa. Por exemplo, podemos repartir o código para não ficar demasiado complexo, do que tentar examinar tudo de uma vez;
b) Análise de código dinâmico: A análise dinâmica de código envolve a depuração do binário suspeito, de uma maneira controlada, para compreender a sua funcionalidade. Para isso, podemos correr partes do código e intercetar as suas comunicações para identificar diferentes estágios.

D. Análise de Memória

A análise de memória visa a procura de vestígios deixados pelo *malware*, onde a integração desta técnica ajuda a perceber o *workflow* do binário após a infecção. É especialmente útil para determinar os recursos furtivos e evasivos do *malware*.

Na escolha das ferramentas para analisar memória volátil, há que ter em conta o programa a usar para fazer o *dump* de memória, visto que é necessário pesar a importância de usar um programa que deixe uma pegada digital menor, mas não permita que o sistema *crashe* com a sua utilização.

Por norma, utiliza-se o *FTK Imager* para fazer o *mount* da memória volátil, porque apesar de deixar uma pegada digital maior que o seu concorrente, o *dump it*, não deita abaixo o sistema tão facilmente. O FTK para além das funcionalidades de *mount* da memória volátil, apresenta outras tantas funções, sendo uma das ferramentas mais utilizadas para informática forense, que para a análise de *software* malicioso não são tão relevantes como aquela que se mencionou.

Para fazer a análise propriamente dita da memória volátil, recorre-se, normalmente, a softwares como o *Volatility*.

A *framework Volatility* é uma ferramenta forense de memória de código aberto mantida pela *Volatility Foundation* que permite aos investigadores extrair artefactos relevantes da memória RAM.

Através das opções de comandos que são possíveis de executar, é possível recolher informação sobre a identificação de tarefas que foram iniciadas por processos suspeitos não nativos do sistema operativo da máquina infetada, determinação do caminho da pasta a partir da qual esse mesmo processo foi executado, bem como as dll's usadas, entre outras informações. [6]

VII. Metodologia de Análise

A. Setup Utilizado

Para a realização do nosso teste, foi necessário criar um *setup*, como se pode observar pela Figura 1, para que se conseguisse testar todas as configurações necessárias num ambiente controlado.

Assim sendo, decidiu-se recorrer à virtualização, através da utilização de um *hypervisor* do tipo 2, o *Virtual Box*, onde foi criada uma máquina virtual com o sistema operativo Windows 10.

Após a instalação deste sistema operativo, com recurso ao *browser* TOR, fez-se o download de uma *sample* de *malware*, através do repositório denominado de "The-MALWARE-Repo" [7], *sample* de *malware* essa, que era referente ao *software* malicioso *WannaCry*.

De seguida, foi na máquina, cujo sistema operativo é o Windows 10, que foi executada a sample de malware descarregada e rapidamente, começou a cifrar a informação que existia na máquina.

No final do processo, apresentou uma nota de resgate, onde o seu conteúdo se pode observar na *Listing* 1 .

Posteriormente, recorremos ao *software* forense *Paladin* e com a ISO deste *software*, fizemos *boot* na máquina infetada.

Seguidamente, procedeu-se ao *mount* da máquina virtual infetada no modo *read only*, para não alterar a integridade da informação, onde se recolheu um conjunto de ficheiros infetados, um ficheiro com extensão txt com a nota de resgate e ainda ficheiros criados pelo próprio software malicioso.

Estes ficheiros foram colocados numa pasta denominada de "*infected*" e recorrendo a uma máquina virtual Kali Linux, foram analisados estes ficheiros de forma estática através das regras *Yara* para nos auxiliar neste processo.

Fig. 1. Imagem ilustrativa do setup utilizado para a realização deste trabalho.

B. Nota de Resgate

Através da observação da nota de resgate recolhida do equipamento infetado, apresentada na listing 1, é possível aferir que o software malicioso em causa trata-se do WannaCry *ransomware*. O *WannaCry* é um exemplo de *ransomware* criptográfico, utilizado pelos cibercriminosos como forma de extorquir dinheiro aos seus alvos.

Para além disso, o pagamento para a desencriptação dos ficheiros é feito em bitcoins, fornecendo-nos o endereço, sendo este, "15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1", para o qual deve ser enviado o pagamento, correspondendo a uma *bitcoin wallet*.

Após a realização do pagamento, é disponibilizado um ficheiro *zip* com o executável responsável pela desencriptação dos ficheiros e, por sua vez, para abrir esse *zip* é necessário colocar uma palavra-passe, sendo esta: wcry123.

```
Q:  What's wrong with my files?
A:  Ooops, your important files are
    encrypted. It means you will not be
    able to access them anymore until they
     are decrypted.
    If you follow our instructions we
        guarantee that you can decrypt all
         your files quickly and safely!
    Let's start decrypting!
Q:  What do I do?
A:  First, you need to pay service fees
    for the decryption.
    Please send $300 worth of bitcoin to
        this bitcoin address: 15
        zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

    Next, please find the decrypt
        software on your desktop, an
        executable file named "!
        WannaDecryptor!.exe".
    If it does not exsit, download the
        software from the address below. (
        You may need to disable your
        antivirus for a while.)

    rar password: wcry123

    Run and follow the instructions!
```

Listing 1. Nota de resgate recolhida da máquina infetada.

C. Análise Estática

Em prol da análise estática do *software* malicioso encontrado, por norma, estabelecem-se um conjunto de objetivos que se pretendem cumprir, sendo estes:

1) Identificar a arquitetura alvo do *malware*;
2) Fingerprint do *malware*;
3) Verificar o binário suspeito;
4) Técnicas de ofuscação usadas para impedir a detecção e a sua análise;
5) Classificação e comparação das amostras de *software* malicioso.

Para responder, da melhor forma, aos objetivos propostos para esta tipologia de análise, uma das ferramentas mais utilizadas para este efeito é a ferramenta Yara.

YARA é uma ferramenta que visa ajudar investigadores de *malware* a identificar e classificar amostras de software malicioso.

Com o YARA, é possível criar descrições de famílias de *malware* (ou o que se quiser descrever), com base em padrões textuais ou binários. Cada descrição ou regra, consiste num conjunto de strings e uma expressão booleana que determina a sua lógica. [8]

A título de exemplo, decidimos testar a ferramenta Yara, sem desprimor para as restantes que serão enunciadas, de modo a entender melhor o seu funcionamento e também colocar em prática aquilo que nos foi ensinado em contexto académico.

Para isso, recorreu-se à utilização do repositório de regras Yara "rules" [9], instalando somente a pasta referente às regras Yara para deteção de *malware* [10].

De seguida, criou-se um *script* [11], de modo a executar todas as regras Yara instaladas, associadas ao diretório da pasta "*Infected*" que continha os ficheiros infetados recolhidos e somente ao ficheiro executável do *software* malicioso, executando o seguinte comando: ./script.pl >/home/kali/Desktop/yara.txt, de modo a perceber se o *output* dava *match* com alguma regra.

Além desta metodologia, ainda se executaram as regras yara sem a utilização do *script*, tanto no diretório da pasta "*Infected*" pasta como no executável, através de comandos com as seguintes opções:

a) r - analisa ficheiros de forma recursiva;
b) s - apresenta as *strings* encontradas no ficheiro;
c) f - acelera o processo pesquisando apenas a primeira ocorrência de cada padrão;
d) n - mostra as regras que não se aplicam;
e) m - mostra os *metadados* associados às regras;
f) w - desativa os *warnings*.

Assim, foram utilizados os seguintes comandos:

a) yara -rsfnmw rules-master/malware/RANSOM-MS17-010-Wannacrypt.yar Infected/WannaCry.exe >>yara1.txt - onde se está a utilizar o comando yara com o ficheiro de regras RANSOM-MS17-010-Wannacrypt.yar diretamente no ficheiro *WannaCry*;
b) yara -rsfnmw rules-master/malware/RANSOM-MS17-010-Wannacrypt.yar Infected >>yara2.txt - onde se está a utilizar o comando yara com o ficheiro de regras RANSOM-MS17-010-Wannacrypt.yar, diretamente no directório *Infected*;
c) yara -s rules-master/malware/RANSOM-MS17-010-Wannacrypt.yar Infected >>yara3.txt - onde se está a utilizar o comando yara com o ficheiro de regras RANSOM-MS17-010-Wannacrypt.yar diretamente no directório *Infected*, utilizando apenas a opção s;

Os outputs obtidos através desta metodologia, encontrar-se-ão disponíveis na secção dos Resultados.

VIII. Resultados

Com base na análise estática efetuada ao *malware* da máquina infetada, conseguiu-se reunir um conjunto de dados relevantes para conseguirmos perceber qual era o software malicioso presente. Para tal, utilizou-se o *script* criado, dando apenas *match* ao ficheiro de regras Yara referente ao *WannaCry*.

Através da análise da *Listing* 2, podemos observar os resultados obtidos do output após executar, com as opções de comandos r, s, f, n, m e w, o ficheiro de regras Yara "RANSOM-MS17-010-Wannacrypt.yar" no ficheiro executável do *malware* encontrado, localizado na pasta "*Infected*".

```
Wanna_Sample_4da1f312a214c07143abeeafb695d
    904
0x125d8:$rwnry: 72 2E 77 72 79
0x37222:$rwnry: 72 2E 77 72 79
Wanna_Cry_Ransomware_Generic
0xeb2c:$s2: WANNACRY
0xefcc:$s3: Microsoft Enhanced RSA and AES
    Cryptographic
0xf2f0:$s5: StartTask
0xf2dc:$s7: 2F 66 00 00 2F 72
0xd3ed:$s8: unzip 0.15 Copyright
wannacry_static_ransom
0xf2f0:$startarg01: StartTask
0xeb2c:$wcry03: WANNACRY
0xf2e5:$fvar01: .wry\x00
```

Listing 2. Output após executar o ficheiro de regras yara RANSOM-MS17-010-Wannacrypt.yar no ficheiro executável, localizado na pasta infected, do malware encontrado.

Ainda sobre a análise estática à *sample* de *malware*, podemos observar, através da *Listing* 3, os resultados obtidos do *output* após executar o mesmo ficheiro de regras Yara, mas agora no diretório da pasta "*Infected*".

```
Wanna_Cry_Ransomware_Generic
0x238:$s1: WannaDecryptor
WannaCry_RansomNote
0x0:$s2: Q: What's wrong with my files?
ransom_telefonica
0x1ced2:$a: RegCreateKeyW
Wanna_Cry_Ransomware_Generic
0x1f06c:$s2: WANNACRY
0x1fd0c:$s3: Microsoft Enhanced RSA and AES
    Cryptographic
0x1aad5:$s8: unzip 0.15 Copyright
wannacry_static_ransom
0x1f06c:$wcry03: WANNACRY
0x1eb55:$fvar01: .wry\x00
wannacry_memory_ransom
0x1eb5c:$s01: %08X.eky
0x1eb94:$s02: %08X.pky
0x1eb68:$s03: %08X.res
0x1eb88:$s04: %08X.dky
Wanna_Cry_Ransomware_Generic
0xeb2c:$s2: WANNACRY
0xefcc:$s3: Microsoft Enhanced RSA and AES
    Cryptographic
0xf2f0:$s5: StartTask
0xf2dc:$s7: 2F 66 00 00 2F 72
0xd3ed:$s8: unzip 0.15 Copyrigh
wannacry_static_ransom
0xf2f0:$startarg01: StartTask
0xeb2c:$wcry03: WANNACRY
0xf2e5:$fvar01: .wry\x00
wannacry_static_ransom
0x0:$wcry03: WANNACRY
```

Listing 3. Output após executar o ficheiro de regras yara RANSOM-MS17-010-Wannacrypt.yar na pasta denominada de infected.

Com base nas *listings* acima apresentadas, conseguimos observar as regras que fizeram correspondência com os ficheiros obtidos da máquina infetada e através dos endereços virtuais de memória que se encontram delineados a vermelho, conseguimos perceber onde foi feita essa correspondência e conseguiram-se, ainda, reunir um conjunto de *strings* que permitiram identificar as várias assinaturas correspondentes ao *sofware* malicioso *WannaCry*.

IX. Conclusão

Com o avanço constante da tecnologia, o aparecimento de novos tipos de *malware* mais persistentes e difíceis de detectar torna-se expectável. O que vai fazer com que exista um aumento na cibercriminalidade, podendo mesmo tornar os ataques com recurso a *software* malicioso num dos principais tipos de crime, se não o principal, comprometendo assim ainda mais a segurança no ciberespaço.

Através da realização deste trabalho, podemos concluir que existem diversas técnicas e ferramentas para analisar *software* malicioso, devendo cada técnica ser aplicada conforme o tipo de análise que se pretende efetuar e ainda devem ser atualizadas com base nos novos perigos que se avizinham, tornando, de certa forma, estas ferramentas intemporais.

De um modo geral, consideramos que o trabalho vai de encontro às expectativas que nos foram propostas aquando da apresentação dos temas em jogo e com isto conseguimos

consolidar melhor os nossos conhecimentos face à análise de *software* malicioso, nomeadamente como proceder à análise do tipo de *malware* em questão, bem como as ferramentas que podem ser utilizadas para tal.

ANEXO A
VÍDEO ILUSTRATIVO

O vídeo seguinte foi criado no âmbito do trabalho proposto para a unidade curricular de Administração Segura de Sistemas Informáticos que se encontra disponível no seguinte link: https://youtu.be/Ew1cXHi-g88.

REFERÊNCIAS

[1] "CNCS - Centro Nacional de Cibersegurança." [Online]. Available: https://www.cncs.gov.pt/

[2] E. C. Centre. (2016) Malware basics. Accessed: 26-01-2022. [Online]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/malwarebasicscomplete.pdf

[3] "Customer Community." [Online]. Available: https://community.mimecast.com/s/article/Content-Examination-Definitions-Using-Fuzzy-Hashing-809049828

[4] "Wireshark · Go Deep." [Online]. Available: https://www.wireshark.org/

[5] markruss, "Process Monitor - Windows Sysinternals." [Online]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/procmon

[6] "Ransomware analysis with Volatility." [Online]. Available: https://resources.infosecinstitute.com/topic/ransomware-analysis-with-volatility/

[7] "The-malware-repo." [Online]. Available: https://github.com/Da2dalus/The-MALWARE-Repo

[8] "YARA - The pattern matching swiss knife for malware researchers." [Online]. Available: https://virustotal.github.io/yara/

[9] "Yara-rules-rules." [Online]. Available: https://github.com/Yara-Rules/rules

[10] "Yara-rules-rules-malware." [Online]. Available: https://github.com/Yara-Rules/rules/tree/master/malware

[11] "Script Perl para correr regras yara - Pastebin." [Online]. Available: https://pastebin.pl/view/5e17130f

Catarina Rodrigues do Nascimento Silva Nasceu em Sintra, Portugal, a 20 de novembro de 1999. Iniciou o mestrado em Cibersegurança e Informática Forense em outubro de 2021. Licenciou-se em Ciências Forenses e Criminais pelo Instituto Universitário Egas Moniz, Portugal, em outubro de 2020, realizando estágio curricular de término da licenciatura na Polícia Judiciária, na UNC3T.

Gonçalo Miguel Conceição Vicente Nasceu em Santarém, Portugal, a 16 de dezembro de 1999. Iniciou o mestrado em Cibersegurança e Informática Forense em outubro de 2021. Licenciou-se em Engenharia Informática (Ramo Tecnologias de Informação) no Instituto Politécnico de Leiria, Portugal em julho de 2021, obtendo 18 valores no Projeto de Informática, onde desenvolveu uma aplicação web denominada *SmartFeedback*.

Atualmente exerce funções de *Web Developer* no Valgrupo desde novembro de 2021.