DOI: 10.5748/20CONTECSI/PSE/SEC/7235

eLocator: e207235

UM ESTUDO COMPARATIVO DAS ESTRATÉGIAS UTILIZADAS POR TROJANS SPYWARES E RANSOMWARES SOB UMA PERSPECTIVA DE ANÁLISE EXPERIMENTAL

Patrick Escórcia Taraborelli – https://orcid.org/0009-0006-2555-3113
Instituto De Pesquisas Tecnológicas - Ipt

Vagner Luiz Gava – https://orcid.org/0000-0001-5965-957X
Instituto De Pesquisas Tecnológicas - Ipt

Anderson Aparecido Alves Da Silva – https://orcid.org/0000-0001-5426-6478
Instituto De Pesquisas Tecnológicas - Ipt

Alessandro Santiago Dos Santos – https://orcid.org/0000-0003-0037-980X
Instituto De Pesquisas Tecnológicas - Ipt

A COMPARATIVE STUDY OF THE STRATEGIES USED BY TROJANS, SPYWARES AND RANSOMWARES FROM AN EXPERIMENTAL ANALYSIS PERSPECTIVE

ABSTRACT

Malware has caused a series of losses in the digital world, as it uses technologies capable of taking advantage of system and user vulnerabilities to cause damage by compromising the confidentiality, integrity or availability of the victim's data, applications or operating system. The present work proposed to investigate the technological strategies used by Trojans, Spywares and Ransomwares, through experimental analysis, identifying the common operating mechanisms and the most exploited vulnerabilities. The CAPE sandbox environment was used to perform the dynamic analysis to observe its behavior at run time. In the analyzes carried out, the behaviors of these malware were identified and then a comparative study was carried out between pairs of malwares belonging to the same type. It was possible to identify common indicators in terms of behavior, such as communication with command and control servers, evasion techniques, and persistence methods. Behavior diagrams were constructed in order to summarize the activities observed in the experiments. It is expected that this diagnosis can contribute to the development of threat detection technologies, incident response strategies, and the development of additional work in the area of cybersecurity.

Keywords: cybersecurity; malware; sandbox; CAPE

UM ESTUDO COMPARATIVO DAS ESTRATÉGIAS UTILIZADAS POR TROJANS, SPYWARES E RANSOMWARES SOB UMA PERSPECTIVA DE ANÁLISE EXPERIMENTAL

RESUMO

Os malwares têm causado uma série de prejuízos no mundo digital, uma vez que utilizam tecnologias capazes de aproveitar-se das vulnerabilidades de sistemas e de usuários para causar prejuízos com o comprometimento da confidencialidade, integridade ou disponibilidade dos dados, aplicativos ou sistema operacional da vítima. O presente trabalho propôs-se a investigar as estratégias tecnológicas utilizadas por Trojans, Spywares e Ransomwares, por meio de análise experimental, identificando os mecanismos de funcionamento comuns e as vulnerabilidades mais exploradas. Foi utilizado o ambiente sandbox CAPE na realização da análise dinâmica para observar o seu comportamento em tempo de execução. Nas análises realizadas, foram identificados os comportamentos desses malwares e, em seguida, realizado um estudo comparativo entre pares de malwares pertencentes ao mesmo tipo. Foi possível identificar indicadores comuns em termos de comportamento, como a comunicação com servidores de comando e controle, técnicas de evasão, e métodos de persistência. Foram construídos diagramas de comportamentos de forma a sintetizar as atividades observadas nos experimentos. Espera-se que esse diagnóstico possa colaborar para o desenvolvimento de tecnologias de detecção de ameaças, com estratégias de resposta a incidentes, e com o desenvolvimento de trabalhos adicionais na área de segurança cibernética.

Palavras-chave:cibersegurança; malware; sandbox; CAPE

1. INTRODUÇÃO

Nas últimas décadas, foram observados o desenvolvimento e o impacto de uma grande profusão de inovações. Cabe destacar o advento dos microprocessadores, da fibra ótica e, principalmente, da internet. Uma era em que uma nova sociedade parece estar emergindo a partir da Transformação Digital, onde ocorrem profundas transformações sociais e tecnológicas, ambas significativamente estimuladas pela incessante e crescente geração de inovações em Tecnologias da Informação e Comunicação (TIC) (WEISS, 2019).

As TIC estão atuando como vetores essenciais para que as inovações aconteçam em todas as áreas da atividade humana, criando novas possibilidades para que indivíduos se relacionem entre si. Nesse contexto, temos uma forma inovadora de criar, promover e difundir a economia da informação, a partir de um novo ecossistema globalmente acessível, onde a sociedade passa a conviver com um novo desafio: o de utilizar com inteligência e adaptar-se ao novo uso da informação, de forma que possa amadurecer e gerar mais valor (WEISS, 2019).

A expansão da conectividade global também permitiu que agentes maliciosos explorassem as vulnerabilidades dos sistemas de informação e se tornassem uma ameaça a ser reconhecida. Em constante evolução, esses agentes frequentemente utilizam-se de artifícios para dificultar sua detecção, como por exemplo técnicas evasivas conforme apresentado por Afianian et al. (2019), e, sua grande diversidade de variantes dificulta as técnicas tradicionais baseadas em assinaturas (GANDOTRA; BANSAL; SOFAT, 2014) (MIRA, 2021).

Nos últimos anos, a expansão do número de computadores nas residências tem aumentado,o que foi impulsionado pela pandemia de SARS-COV2, e houve uma grande mudança de hábitos, com a expansão do teletrabalho e da telescola, sendo acompanhada por um grande crescimento nos crimes cibernéticos. Parte considerável desse crescimento se deve pela maior exposição dos dispositivos pessoais e pela não utilização de boas práticas de cibersegurança (TERESO; PRATAS, 2021).Esses agentes vão atuar frequentemente no comprometimento de algum serviço de segurança da informação (KUNWAR; SHARMA, 2016), causando prejuízos nos princípios básicos de segurança: Confidencialidade, Integridade, Disponibilidade e Autenticação, não somente nas residências, mas também no ambiente corporativo.

No contexto brasileiro, o CERT.br (2023), órgão vinculado ao NIC.br, concentrou-se na divulgação on-line dos materiais para a conscientização e de boas práticas por meio da Cartilha de Segurança para Internet. Com o cenário de pandemia, no qual as escolas suspenderam as aulas presenciais levando as crianças e os jovens a ficarem mais tempo em frente às telas, o CERT.br desenvolveu material para permitir material mais lúdico, com uma classificação dos tipos de malwares (Quadro 1), que poderia atingir um público mais jovem que estavam utilizando os seus dispositivos em casa enquanto aprendiam mais sobre agentes maliciosos e mecanismos de defesa.

Cada tipo tem seus próprios métodos de propagação e mecanismos para explorar vulnerabilidades, no entanto um malware podem combinar diversas tecnologias para atingir os seus objetivos, muitas vezes utilizando de diversas técnicas combinadas para infecção, propagação e ações funcionais.

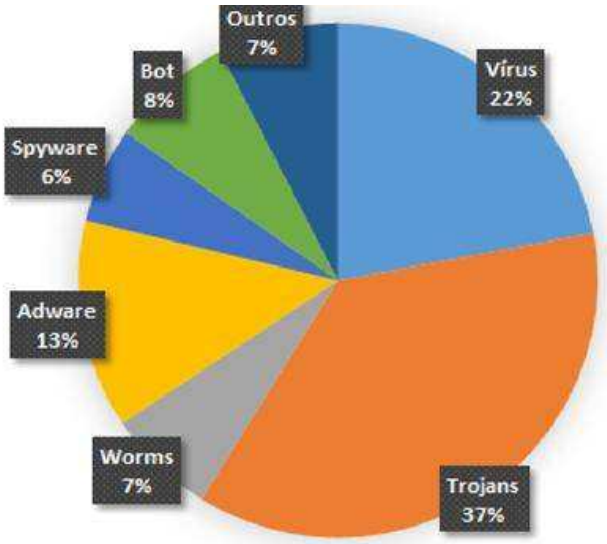
Quadro 1. Tipos de malwares

Vírus 	Se comporta de maneira semelhante a um vírus biológico. Ele se anexa a arquivos ou programas legítimos e, quando esses arquivos são executados, o vírus também é ativado. Uma das características definidoras dos vírus é sua capacidade de se replicar e se espalhar para outros arquivos e sistemas.	**Bots** 	Obtém acesso a dispositivos por meio de uma codificação maliciosa, e o invasor pode utilizar os recursos computacionais da vítima em uma rede contendo outros dispositivos infectados, conhecida como botnet. Eles podem ser controlados remotamente para executar ações coordenadas
Trojans 	Programas maliciosos disfarçados como software legítimo ou atraente para enganar os usuários a baixá-los ou instalá-los. Ao contrário dos vírus, os trojans não se replicam sozinhos. Uma vez instalados, são capazes de instalar outros malwares no sistema infectado.	**Spywares** 	Malware projetado para coletar informações pessoais e confidenciais de um sistema sem o conhecimento ou consentimento do usuário. Ele pode rastrear atividades online, como histórico de navegação, digitação de teclado, senhas e informações financeiras, e enviar esses dados a terceiros maliciosos.
Ransomwares 	Bloqueiam o dispositivo da vítima ou criptografam os seus dados. Normalmente é exigido um resgate para restaurar o acesso. As informações para o pagamento costumam ser disponibilizadas em um arquivo de texto (ransom note) e o pagamento costuma ser exigido com a utilização de criptomoedas.	**Rootkits** 	Se infiltram profundamente no sistema operacional, geralmente obtendo privilégios de administrador (root) para ocultar sua presença. Eles são usados para esconder outros malwares no sistema e garantir acesso persistente para os invasores. Detectar e remover rootkits é desafiador devido à sua capacidade de camuflagem e ao fato de operarem no nível mais profundo do sistema.
Backdoors 	Criam pontos de acesso ocultos ou vulnerabilidades em um sistema permitindo o acesso não autorizado. A detecção e remoção de backdoors podem ser complexas, uma vez que são projetados para operar silenciosamente e evitar a detecção.	**Worms** 	Tem a capacidade de se replicarem. No entanto, esses programas maliciosos autônomos não necessitam de interação do atacante ou da vítima para se multiplicarem. Eles exploram vulnerabilidades de softwares para se replicar e podem se espalhar rapidamente, consumindo largura de banda de rede e normalmente causando congestionamentos.

Fonte: Adaptado de CERT.br (2023)

Segundo AVAST (2022), o malware predominante no Brasil é pertencente ao grupo de Trojans, seguido por demais tipos, como apresentado naFigura *1*.

Figura 1. Malwares mais predominantes no Brasil



Fonte: Adaptado de Avast (2022)

Os resultados encontrados estão em concordância com o relatório de segurança publicado por ESET (2022), onde confirmam a liderança dos malwares do tipo trojan no cenário brasileiro atual. Outros destaques são o tipo Spyware, o qual têm apresentado uma tendência de crescimento no último ano (OXFORD ANALYTICA, 2023); e o Ransomware, o qual tem se figurado com grande frequência na mídia devido ao impacto causado em grandes corporações (SECURITY REPORT, 2023).

Torna-se assim imperativo que as técnicas utilizadas pelos agentes maliciosos sejam estudadas de forma a minimizar a superfície de ataque das vulnerabilidades existentes nos sistemas de informação.Este trabalho pretende avaliar os mecanismos utilizados pelos principais tipos de malwares que atacam o cenário brasileiro, a fim de identificar padrões e estratégias de infecção e proliferação dos malwares, os quais podem formar uma base de conhecimento para serem utilizados em mecanismos de mitigação dos riscos e impactos.

2. MATERIAIS E MÉTODOS

Para atingir os objetivos de analisar os mecanismos utilizados pelos principais malware, optou-se uma por uma abordagem de métodos experimentais, que executam experimentos e avaliam os comportamentos e características do ambiente experimentado. Assim, a metodologia empregada procurou reunir informações dos principais tipos de malwares e das vulnerabilidades exploradas por esses, através da realização de experimentos, em um ambiente laboratorial de análise de malwares, os quais estão detalhados nas subseções de Materiais e Métodos, e na seçãoResultados e discussão.

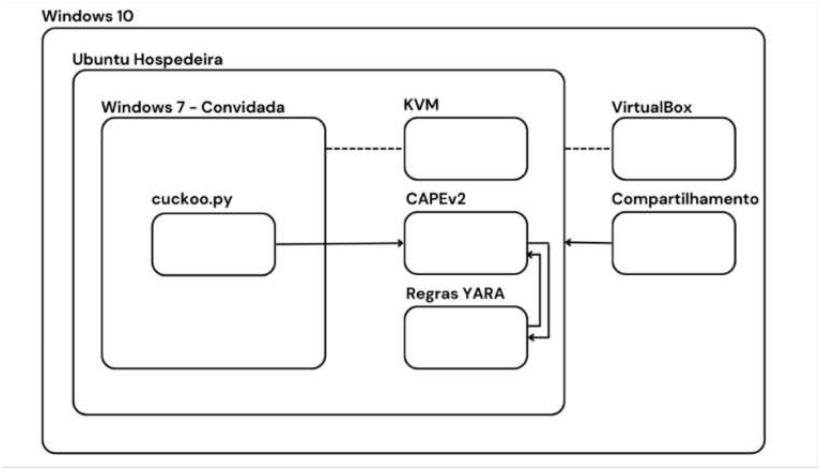
2.1. Materiais

O trabalho foi desenvolvido em um ambiente de análises de malware, composto por computador, software de virtualização, amostras de malwares e ferramentas de análises.

- O computador de execução foi um Notebook Lenovo ThinkPad com Processador: AMD Ryzen 5 5500U, Memória: 16GB DDR4 , Armazenamento: 1TB SSD.
- Software de virtualizaçãoOracle VM VirtualBox 7.0.10 e KVM (Kernel-based Virtual Machine);
- Sistemas operacionais dos ambientes foram: VM Ubuntu 22.04 LTS e Windows 7 Professional 64b.
- Ferramentas de análise CAPEv2 Sandbox,
- MS Office 2016, Python 3 32 bits e o PowerShell 5.1.

A configuração final do ambiente sandbox seguiu o esquema ilustrado na Figura 2.

Figura 2. Arquitetura conceitual do ambiente de teste



Fonte: Elaborado pelos autores

O ambiente contendo o Sistema Operacional (SO) Ubuntu, que chamaremos de máquina virtual hospedeira, foi virtualizado com o VirtualBox, e o ambiente contendo o SO Windows 7, que chamaremos de máquina virtual convidada, foi virtualizado com o KVM. Essa configuração permitiu que a ferramenta CAPE, instalado na máquina virtual hospedeira, conseguisse analisar o comportamento da máquina virtual convidada, por meio da execução do script cuckoo.py, disponibilizado na plataforma GitHub por Rebaker (2023). O Quadro *2* apresenta as configurações das maquinas virtuais.

O CAPE consegue identificar diversos padrões de comportamentos utilizando as regras Yara. Essas regras são escritas em uma sintaxe específica para identificar padrões a serem pesquisados e identificados.

Quadro 2. Configuração da máquina virtual hospedeira

1.	**VM Ubuntu 22.04 LTS,** 4 CPUs, Memória: 8092 MB, Disco rígido virtual: 50 GB. Recursos estendidos habilitados: Habilitar VT-x/AMD-V Aninhado; e Virtualização de Hardware: Habilitar Paginação Aninhada
2.	**VM Windows 7 Professional 64b,** 2 CPUs, Memória: 4096 MB, Disco rígido virtual: 50 GB

Fonte: Elaborado pelos autores.

Para a realização das atividades experimentais foram selecionadas duasamostras de cada um dos três tipos de malware (Trojan, Spyware e Ransoware) conforme oQuadro *3*.

Quadro 3. Trojans utilizados no experimento

Tipo	Família	Hash - SHA 256
Trojan	AgentTesla	0157c83047900d2fd372d845d5107e403b7485aa00c3a7b762121f19bdf8b45e
Trojan	SmokeLoader	87026781f4f06f6b871d504bfc7d31876085265e4364ebc4a2b673f18c5e9a19
Spyware	Snake	02c7c03ceb187b25fe31e9a6996ebab1008f587512ab451836c2eef6c7411bea
Spyware	Formbook	2334ecedc27e808bbf63a9c3813298d6605d227c6c9f01a8f1f5a636f8439436
Ransoware	WannaCry	be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844
Ransoware	STOP/Djvu	b03dd67bfc32132c63da78e037f5ffa6093275f3c81ebf68cd10073bd1b9bcd5

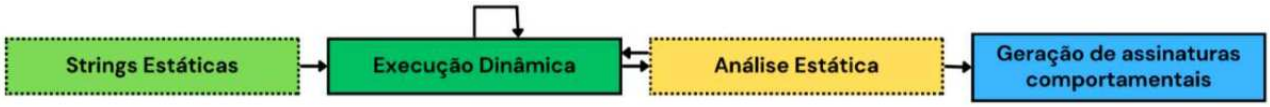
Fonte: Elaborado pelos autores a partir das amostras coletadas em Malwarebazaar (2023).

2.2. Métodos

Como ferramenta de coleta e análise do comportamento do malware foi utilizada a ferramenta CAPE Sandbox, um ambiente baseado no CuckooSandbox. Trata-se de um ambiente open sourcecontrolado e monitorado que utiliza regras Yara para a detecção de padrões comportamentais dos malwares.

Foram levadas em consideração, as observações que um fluxo de trabalho deve seguir ao realizar a análise de malwares, propostas por Wong et al (2021), sendo adotado o fluxo de trabalho mais utilizado pelos analistas participantes da pesquisa descrita no artigo (Figura 3).

Figura 3. Fluxo de trabalho de análise de malwares



Fonte: Adaptado de Wong et al (2021)

As caixas com bordas pontilhadas representam etapas opcionais de serem realizadas durante o fluxo de trabalho de análise de malwares.

As etapas Strings Estáticas e Análise Estática, onde são realizadas a análise estática do objeto de estudo, não foram realizadas neste trabalho.

Durante a etapa Execução dinâmica, podem ocorrer diversas iterações, onde o analista pode realizar alterações no ambiente virtual e/ou nas amostras de malwares que estão sendo estudadas.

A etapa representada com uma caixa azul, a etapa de Geração de assinaturas comportamentais, representa o objetivo principal a ser alcançado no fluxo de trabalho.

2.2.1. Configuração do ambiente sandbox de análise de malwares

Nesta seção será detalhada a configuração utilizada no ambiente sandbox e a sua implementação, onde teremos a seleção do sistema operacional e a seleção dos malwares utilizados com as suas respectivas justificativas.

2.2.2. Seleção do sistema operacional

O ambiente analisado foi o Windows 7 Professional. Esse Sistema Operacional (SO) está a muitos anos no mercado, de forma que suas vulnerabilidades foram extensamente estudadas.

Esse SO não possui mais o suporte base (encerrado em 13/01/2015), o suporte estendido (encerrado em 14/01/2020) ou o suporte estendido para empresas (encerrado em 10/01/2023) da empresa Microsoft, o que significa que as suas vulnerabilidades não estão sendo corrigidas atualmente pela sua empresa desenvolvedora (MICROSOFT, 2023).

É o SO com maior número e variedade de malwares, e ainda possui uma grande base de usuários, atualmente com 49,14 milhões (STATCOUNTER, 2023). O número de usuários do SO Linux, para termos uma comparação, está atualmente em torno de 32,8 milhões (STATISTA, 2023), não considerando os usuários do sistema Android.

Além disso, o Windows Server 2008 R2, o qual está presente em mais de 50 mil empresas (ENLYFT, 2023), é um SO variante do Windows 7, possuindo vulnerabilidades análogas.

2.2.3. Seleção dos malwares

Mesmo entre malwares de um mesmo tipo, existem diferenças comportamentais entre eles, sendo possível classificar esses agentes em famílias. As famílias escolhidas para o estudo são as famílias mais frequentemente encontradas, segundo o Malwarebazaar (2023), o qual é o site onde foram obtidas as amostras de malwares utilizados nesse trabalho.As amostras utilizadas podem ser baixadas diretamente do site, utilizando o hash SHA 256 correspondentes de cada amostra.

2.2.4. Implementação do ambiente sandbox

Primeiramente, preparamos o ambiente de análise isolando uma VM no SO Ubuntu, utilizando o software VirtualBox. Foi escolhida a utilização do ambiente sandbox CAPE, com as VMs configuradas de acordo com oQuadro 2 descritos na seção de materiais. A documentação oficial pode ser encontrada no site da ferramenta (CAPE, 2023).

A instalação e execução do CAPE foi realizada nesta máquina virtual seguindo os procedimentos detalhados no tutorial disponibilizado na plataforma GitHub por Rebaker (2023).

Após a execução dos passos de instalação do script apresentado no GitHub, foi necessário configurar a rede virtual entre as VMs que foram objeto de análise. O CAPE foi acessado pelo browser Firefox pela porta 8080 do endereço localhost (http://127.0.0.1:8080).

Na máquina virtual convidada foi necessário desativar o firewall e outros mecanismos de proteção, conforme indicado no tutorial disponibilizado no GitHub (REBAKER, 2023).

2.2.5. Execução dos experimentos

Após o isolamento do ambiente com a implementação do ambiente sandbox, criamos um snapshot da máquina virtual convidada.

Em seguida, executamos um dos malwares no ambiente controlado, seguindo a ordem do Quadro *3*apresentado nasubseção Materiais. Após o registro das atividades pelo CAPE, foi restaurado o snapshot da máquina virtual convidada, de forma a permitir a execução do malware seguinte.

Durante a execução dos malwares, o CAPE capturou informações sobre as atividades dos malwares como criação de arquivos, a modificação do Registro do Windows, chamadas de sistema e tráfego de rede.

3. RESULTADOS E DISCUSSÃO

Nesta seção serão apresentados os resultados obtidos nos ambientes virtualizados, a partir do qual serão construídos diagramas comparativos dos comportamentos apresentados pelos malwares estudados.

O CAPE utiliza as regras Yara para identificar características específicas, como sequências de bytes, strings, funções hash, ou comportamentos específicos, de acordo com as condições lógicas definidas pelo programador da regra.

As cores representadas nas assinaturas encontradas nos resultados da Figura *4*, Figura *8* e Figura *10*, que indicam o potencial de severidade do comportamento encontrado, e são definidas na programação das regras. A cor azul representa um potencial menor, a cor laranja um potencial moderado e a cor vermelha um potencial elevado. Esta forma de apresentação dos resultados pode colaborar para reduzir o número de falsos-positivos detectados durante a análise e com a visualização do funcionamento do objeto de análise. Os detalhes de criação e edição de assinaturas podem ser encontrados na documentação do site do CAPE (2020).

A instalação e execução do CAPE foi realizada nesta máquina virtual seguindo os procedimentos detalhados no tutorial disponibilizado no GitHub por Rebaker (2023).

As assinaturas presentes na Figura *4*, Figura *8* e Figura *10*que forem citadas no texto deste trabalho estarão identificadas com letras maiúsculas, referindo-se à Figura de sua respectiva subseção.

3.1. Laboratório – Trojans

Os resultados da execução da ferramenta CAPE para os malwares AgentTesla e SmokeLoader podem ser observados na Figura 4.

Figura 4. Assinaturas detectadas pelo CAPE no experimento de Trojans



Fonte: Elaborado pelos autores.

Foi possível observar algumas semelhanças entre os malwares: ambos são do tipo Trojan, possuindo funcionalidades de se disfarçar como software legítimo para enganar os usuários.

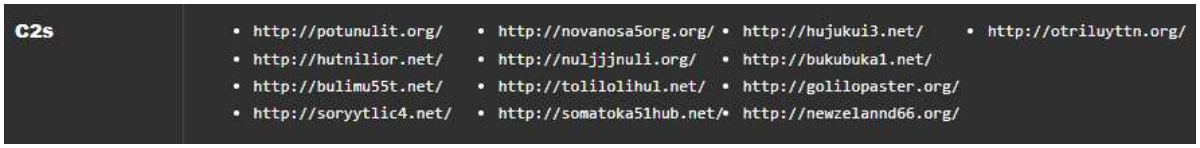
A maioria dos malwares utilizados neste trabalho acionaram as regras identificadas com as letras **A** e **B**. A primeira está relacionada com a utilização de uma função da API do

Windows que realiza tratamentos de exceção em um programa em execução, que pode ser utilizado para dificultar a detecção do malware. A segunda buscou identificar os endereços dos adaptadores, o que pode potencialmente ser utilizado para detectar redes virtuais e falhou. Além disso, observou-se outra semelhança em que a maioria dos malwares também alocou espaço de memória com permissões de leitura escrita e execução – RWX (**F**).

O AgentTesla realizou quatro requisições utilizando o protocolo HTTP que falharam no experimento (**C**). Em seguida o malware estabeleceu uma conexão HTTPS que foi bem-sucedida (**D**). Após o download por meio de um script powershell, ocorreu a execução do arquivo binário "kxjbzogon.exe" (**E**).Em seguida, ele iniciou uma série de processos relacionados a captura de informações do computador infectado.

O SmokeLoader tentou identificar a presença do antivírus Avast (**G**) e de um ambiente sandbox (**H**) através da busca da presença bibliotecas específicas. Ambas as tentativas falharam, retornando "DLL_NOT_FOUND". Em seguida o malware realizou técnicas de evasiva de detecção eutilizou o método POST, utilizando a porta 80, para estabelecer conexões HTTP com os seus Servidores de Comando e Controle - C2s (**I**). A figura abaixo (Figura 5) lista os endereços utilizados.

Figura 5. Endereços C2s utilizados pelo malware SmokeLoader



Fonte: Elaborado pelos autores.

Conforme a Figura 6, verificou-se que ambos utilizam técnicas de ofuscação com o empacotamento de seus arquivos executáveis, acionando as seguintes Regras Yara: "INDICATOR_EXE_Packed_GEN01" no malware AgentTesla e "embedded_pe" no malware SmokeLoader. No AgentTesla ainda se observou o acionamento da Regra Yara "HeavensGate", a qual se refere a uma forma evasiva onde o malware busca executar instruções em um modo de arquitetura de 32 bits em sistemas de 64 bits (**J**).

Figura 6. Detalhe de assinatura dos malwares AgentTesla e SmokeLoader respectivamente



Fonte: Elaborado pelos autores

Com os resultados obtidos no ambiente sandbox, foi possível construir um diagrama para os Trojans analisados (Figura 7).

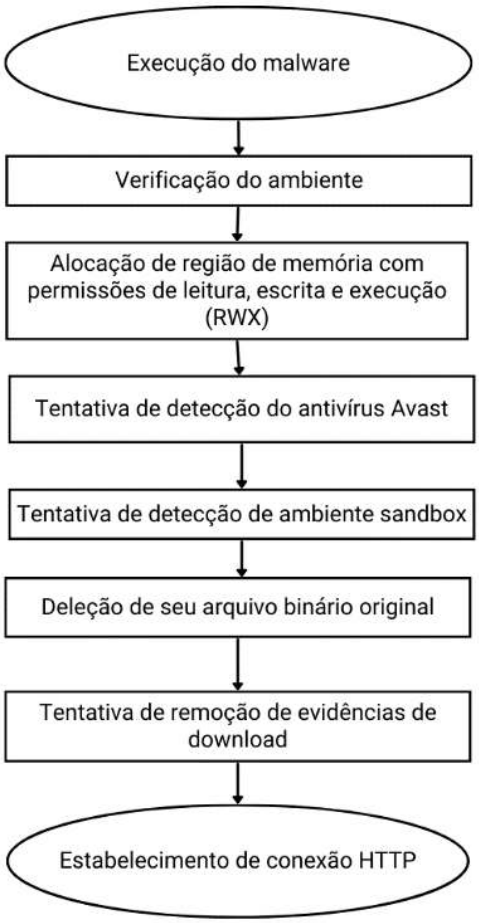
Em resumo, verificamos que o AgentTesla possui funcionalidades de roubar informações diretamente, possuindo também características de Spyware. O SmokeLoader, por ser um trojan downloader, possui funcionalidades de introdução de novas ameaças, possuindo também características de backdoor.

Figura 7. Diagramas dos comportamentos dos Trojans analisados

AgentTesla



SmokeLoader



Fonte: Elaborado pelos autores.

3.2. Laboratório – Spywares

Os resultados da execução da ferramenta CAPE para os malwares Snake e Formbook podem ser observados na Figura 8.

Foi possível observar algumas semelhanças entre os malwares: ambos são malwares do tipo spyware, o que significa que ambos possuem a capacidade de coletar informações sensíveis dos sistemas infectados.

Observou-se um comportamento inicial semelhante entre eles e também semelhante ao laboratório de trojans realizado anteriormente, onde os malwares verificaram o ambiente em que estão inseridos, de forma a obterem informações que possam direcionar as suas atividades (**A**). Em seguida, foi observado também um comportamento semelhante entre os malwares para ofuscar suas atividades (**B**). Semelhantemente, ambos também alocam espaço de memória com permissões de leitura, escrita e execução – RWX.

Quanto as diferenças, foi observado que o Snake estabeleceu uma conexão com um host remoto (**D**) para o envio futuro de dados capturados do computador hospedeiro (**E**). Já o Formbook realizou injeção de código (**F**) e deletou seus próprios arquivos (**G**), provavelmente como forma evasiva para dificultar a sua detecção.

Figura 8. Assinaturas detectadas pelo CAPE no experimento de Spywares



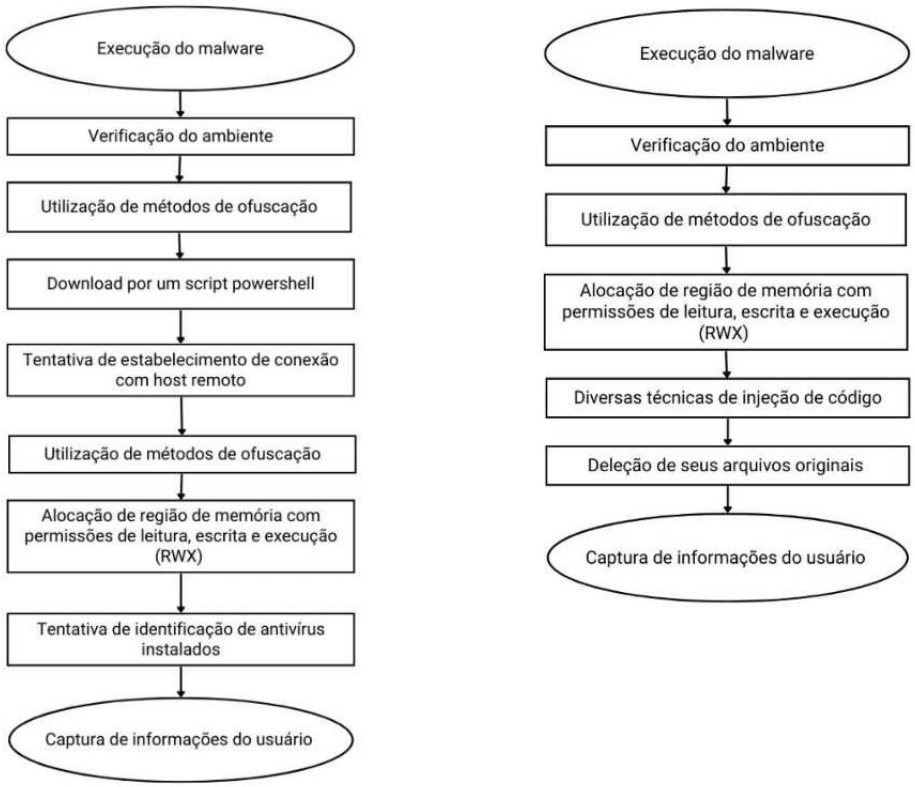
Fonte: Elaborado pelos autores.

Com os resultados obtidos no ambiente sandbox, foi possível construir um diagrama para os Spywaresanalisados (Figura 9).

Em resumo, verificamos que os spywares utilizaram mecanismos diferentes para atingirem os seus objetivos. O Snake buscou estabelecer conexão HTTP com um host remoto no início do seu comportamento, antes de capturar os dados do computador hospedeiro, e o Formbook realizou diversas técnicas de injeção de código e de ofuscação para atingir o seu objetivo.

Figura 9. Diagramas dos comportamentos dos Spywares analisados

Snake **Formbook**



Fonte: Elaborado pelos autores.

3.3. Laboratório – Ransomwares

Os resultados da execução da ferramenta CAPE para os malwares WannaCry e STOP/Djvu podem ser observados na Figura 10.Foi possível observar algumas semelhanças entre os malwares: ambos são do tipo ransomware, possuindo funcionalidades de realizar a criptografia dos arquivos no sistema do usuário.

No WannaCry, foram identificadas tentativas de conexão com um endereço IP e porta que não estavam mais ativos (**A**), possivelmente como parte de uma tentativa de comunicação com servidores de Comando e Controle (C2s) que já estavam offline. Em seguida, após uma verificação do ambiente, o malware utilizou APIs do Windows para gerar uma chave criptográfica (**B**). Na sequência, observou-se a exclusão de uma grande quantidade de arquivos (**C**), com 1413 arquivos deletados no total. Esse comportamento pode ter ocorrido para ocultar rastros ao deletar os logs e modificar as configurações do sistema para permitir a instalação de módulos adicionais do malware.

Ocorreu em seguida a execução do arquivo binário !WannaDecryptor!.exe (**D**) e do script (c.vbs) (**E**) que deram continuidade às ações do malware. O WannaCry realizou a criptografia de diversos arquivos (**F**) utilizando a chave criptográfica criada anteriormente (**B**). Ocorreu a tentativa de mudança do papel de parede de área de trabalho (**G**) que não foi bem-sucedida no experimento. Normalmente malwares desse tipo modificam o papel de parede da área de trabalho e/ou criam arquivos que contenham instruções para o depósito de criptomoedas para, de acordo com os atacantes, obter o acesso aos dados criptografados.

Quanto ao STOP/Djvu, foram observadas tentativas de conexões HTTP (**H**) e HTTPS (**I**), possivelmente para se comunicar com servidores remotos. Foi verificado a realização diversas técnicas de injeção de código (**J**) e sua configuração para ser executado

automaticamente na inicialização do Windows (**K**), o que é uma técnica comum de persistência.

Quanto às diferenças no resultado criptográfico, verificou-se que o WannaCry utilizou técnicas de criptografia que exploraram uma vulnerabilidade no protocolo SMB (Server MessageBlock) do Windows. O método criptográfico do STOP/Djvu não foi identificado pelas assinaturas do ambiente sandbox, o que indica que provavelmente foram utilizadas chaves offline para a criptografia.

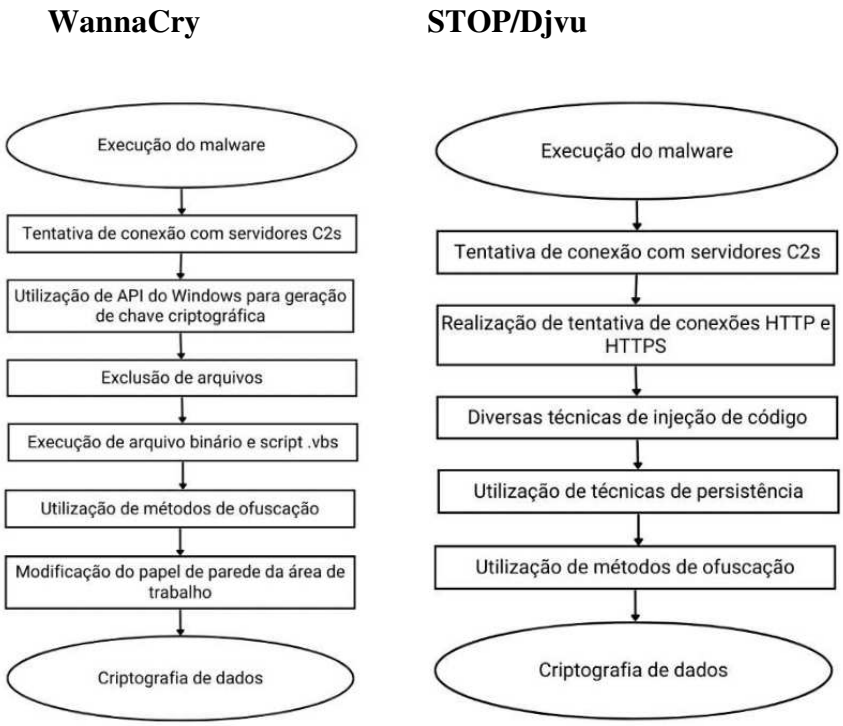
Figura 10. Assinaturas detectadas pelo CAPE no experimento de Ransomwares



Fonte: Elaborado pelos autores.

Com os resultados obtidos no ambiente sandbox, foi possível construir um diagrama para os Ransomwares analisados (Figura 11).

Figura 11. Diagramas dos comportamentos dos Ransomwares analisados



Fonte: Elaborado pelos autores.

4. CONCLUSÕES

O trabalho desenvolvido apresentou, por meio de análise experimental, o comportamento dos malwares pertencentes aos tipos Trojans, Spywares e Ransomwares e realizou uma comparação de suas características entre os malwares pertencentes ao mesmo tipo, de forma a evidenciar os seus comportamentos semelhantes e as suas diferenças.

A análise revelou uma notável diversidade nas táticas e técnicas empregadas pelos malwares dentro do mesmo tipo, o que destaca a adaptabilidade dos desenvolvedores de malwares, que podem utilizar abordagens distintas mesmo dentro de uma mesma categoria.

Os objetivos propostos no trabalho foram atingidos com os resultados obtidos, onde foi possível identificar indicadores comuns em termos de comportamento, como a comunicação com servidores de comando e controle, técnicas de evasão, e métodos de persistência. Foram identificados padrões, estratégias de infecção e a forma como as proliferações dos malwares estudados ocorrem.

Foi observado também a importância de uma abordagem holística na análise de malwares. Uma análise mais completa, envolvendo análise estática e a utilização de ferramentas adicionais pode colaborar para a identificação das atividades desempenhadas pelo malware e auxiliar na construção de um diagrama de comportamento mais completo.

Trabalhos futuros podem abordar a utilização de ambientes sandbox com características diferentes das abordadas nesse trabalho, de forma a complementar a avaliação comportamental dos malwares estudados. Nesses trabalhos, podem ser utilizados softwares adicionais para a verificação das atividades dos malwares, ou pode ser realizada a alteração de outros parâmetros, como por exemplo o SO utilizado.

Espera-se que esse estudo contribua para trabalhos futuros, onde seja possível a elaboração de estratégias de mitigação e correção de vulnerabilidades, favorecendo a construção de um ambiente informatizado mais seguro.

5. REFERÊNCIAS BIBLIOGRÁFICAS

AFIANIAN, Amir; NIKSEFAT, Salman; SADEGHIYAN, Babak; BAPTISTE, David. Malware Dynamic Analysis Evasion Techniques. **Acm Computing Surveys**, [S.L.], v. 52, n. 6, p. 1-28, 14 nov. 2019. Association for Computing Machinery (ACM). http://dx.doi.org/10.1145/3365001.

AVAST. **Trojans e adware são os tipos de malware mais disseminados no Brasil**. 2022. Disponível em: https://press.avast.com/pt-br/trojans-e-adware-sao-os-tipos-de-malware-mais-disseminados-no-brasil. Acesso em: 07 set. 2023.

CAPE. **CAPE Sandbox Book**. 2023. Disponível em: https://capev2.readthedocs.io/en/latest/. Acessoem: 30 set. 2023.

CAPE. **Signatures**: cape sandbox v2.1 book. CAPE Sandbox v2.1 Book. 2020. Disponível em: https://capev2.readthedocs.io/en/latest/customization/signatures.html. Acesso em: 31 out. 2023.

CERT.br. **Códigos Maliciosos**: cartilha de segurança para internet. Cartilha de Segurança para Internet. 2023. Disponível em: https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acesso em: 07 set. 2023.

ENLYFT. **Companies using Windows Server 2008**. 2023. Disponível em: https://enlyft.com/tech/products/windows-server-2008. Acesso em: 09 set. 2023.

ESET. **Security Report: Brasil 2022**. 2022. Disponível em: https://web-assets.esetstatic.com/wls/pt/artigos/relatorios/ESET_Security_Report_Brasil.pdf. Acesso em: 21 set. 2023.

GANDOTRA, Ekta; BANSAL, Divya; SOFAT, Sanjeev. Malware Analysis and Classification: a survey. **Journal Of Information Security**, [S.L.], v. 05, n. 02, p. 56-64, 2014. Scientific Research Publishing, Inc..http://dx.doi.org/10.4236/jis.2014.52006. Disponível em: https://www.scirp.org/journal/paperinformation.aspx?paperid=44440. Acessoem: 08 jul. 2022.

KUNWAR, Rakesh Singh; SHARMA, Priyanka. Malware Analysis. **Proceedings Of The Second International Conference On Information And Communication Technology For Competitive Strategies**, [S.L.], p. 1-4, 4 mar. 2016. ACM. http://dx.doi.org/10.1145/2905055.2905361.

MALWAREBAZAAR. **Statistics**. 2023. Disponível em: https://bazaar.abuse.ch/statistics/. Acesso em: 20 jul. 2023.

MICROSOFT. **Fim do suporte para o Windows 7 e os Aplicativos do Microsoft 365**. 2023. Disponível em: https://learn.microsoft.com/pt-br/deployoffice/endofsupport/windows-7-support. Acessoem: 09 set. 2023.

MIRA, Fahad. A Systematic Literature Review on Malware Analysis. **2021 Ieee International Iot, Electronics And Mechatronics Conference (Iemtronics)**, [S.L.], p. 1-5, 21 abr. 2021. IEEE. http://dx.doi.org/10.1109/iemtronics52119.2021.9422537.

OXFORD ANALYTICA. **Global spyware industry will expand despite scrutiny**. **Emerald Expert Briefings**, [S.L.], p. 1-12, 17 abr. 2023. Emerald. http://dx.doi.org/10.1108/oxan-db278436.

REBAKER501. **CAPEv2 Sandbox Installation**. 2023. Disponívelem: github.com/rebaker501/capev2install/blob/main/readme.md. Acessoem: 30 set. 2023.

SECURITY REPORT. **1800 empresas já foram vítimas de ransomwares em 2023**. 2023. Disponível em: https://www.securityreport.com.br/cerca-de-1800-empresas-ja-foram-vitimas-de-ransomwares-em-2023/. Acessoem: 07 set. 2023.

STATCOUNTER. **Desktop Windows Version Market Share Worldwide**. 2023. Disponível em: https://gs.statcounter.com/windows-version-market-share/desktop/worldwide. Acesso em: 31 ago. 2023.

TERESO, Marco; PRATAS, António. CIBERSEGURANÇA E TELETRABALHO: UM MUNDO DE OPORTUNIDADES DE RISCO. **Atas do VII Encontro Científico da Ui&D (Ecui&D 21)**, Santarém, Portugal, v. 21, n. 7, p. 126-136, 18 jun. 2021.

WEISS, Marcos Cesar. Sociedade sensoriada: a sociedade da transformação digital. **Estudos Avançados**, [S.L.], v. 33, n. 95, p. 203-214, jan. 2019. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/s0103-4014.2019.3395.0013. Disponível em: https://www.scielo.br/j/ea/a/jPn3NkF6dYx8b56V8snsnQf/?format=pdf&lang=pt. Acessoem: 08 jul. 2022.

WONG, Miuyin Yong; LANDEN, Matthew; ANTONAKAKIS, Manos; BLOUGH, Douglas M.; REDMILES, Elissa M.; AHAMAD, Mustaque. An Inside Look into the Practice of Malware Analysis. **Proceedings Of The 2021 AcmSigsac Conference On Computer And Communications Security**, [S.L.], p. 3053-3069, 12 nov. 2021. ACM. http://dx.doi.org/10.1145/3460120.3484759.