Nome: _____ Data: _____ Pontuação: _____

Análise de software malicioso e mitigação de ameaças Guia

Cavalos de Troia, ransomware, spyware, rootkits, sandboxes de virtualização, contenção

VISÃO GERAL DE APRENDIZAGEM SOBRE ANÁLISE DE SOFTWARE MALICIOSO

PROTEGIDO
ENCRIPTAÇÃO DE DADOS
Norma AES de 256 bits

CONFORME
NORMAS GLOBAIS
Referenciais RGPD (GDPR) e CCPA

ZERO-TRUST
POLÍTICA DE ACESSO
Autenticação multifator

Bem-vindo! Este conjunto de atividades guia-te pela análise e prevenção de malware. Vais explorar spyware, trojans, cargas úteis de ransomware, ferramentas de engenharia inversa, comportamento de rootkits e estratégias de contenção.

PONTOS DE CONTROLO DA FICHA DE TRABALHO

- [ ] **Partes 1-4: Domina a cibersegurança e a prevenção de ameaças.**
- [ ] **Partes 5-7: Resolve puzzles de palavras cruzadas e sopas de letras.**
- [ ] **Partes 8-9: Resolve estudos de caso e o desafio de cifra.**
- [ ] **Parte 10: Revê as páginas de perguntas frequentes básicas e avançadas.**
- [ ] **Parte 11: Explora 10 factos interessantes do mundo real.**
- [ ] **Bónus: desafio Pensa rápido.**

Abrir o Guia de Cibersegurança da VPN.com

URL: https://www.vpn.com/pt/ciberseguranca/malware/

O teu roteiro de aprendizagem sobre mitigação de software malicioso

- Distingue os tipos de malware Trojan, worm e rootkit.
- Implementa a execução virtualizada em sandbox para análise de código.
- Concebe planos de contenção e de higienização para cargas de ransomware ativas.

INSTRUÇÕES DO GUIA DE ANÁLISE DE SOFTWARE MALICIOSO

Responde às perguntas de escolha múltipla e de verdadeiro/falso, completa as frases de preencher espaços com o banco de palavras, associa as definições e resolve as palavras cruzadas e a sopa de letras. Aplica os teus conhecimentos à mitigação de software malicioso. Termina com a atividade bónus Pensa rápido.

ANÁLISE DE SOFTWARE MALICIOSO E CONTENÇÃO DE AMEAÇAS (INTRODUÇÃO)

O código malicioso, como cavalos de Troia, worms e ransomware, representa ameaças de grande impacto para terminais e servidores. As equipas de segurança analisam o software malicioso em sandboxes virtuais e aplicam rapidamente controlos de isolamento de rede para conter a propagação da carga maliciosa.

LÊ CADA PONTO DE CONTROLO COM ATENÇÃO E ESCOLHE OU ESCREVE A RESPOSTA CORRETA.

Ponto de controlo 1: Desafio de escolha múltipla

1 **1. Qual é a característica definidora de um cavalo de Troia?**

- A. Disfarça-se de software legítimo para enganar os utilizadores e levá-los a executá-lo
- B. Replica-se automaticamente através das linhas da rede local
- C. Infeta ficheiros dentro de sandboxes virtuais isoladas
- D. Interceta o tráfego do fornecedor de serviços de internet

2 **2. Que tipo de malware encripta ficheiros e exige pagamento?**

- A. Ransomware
- B. Spyware
- C. Rootkit
- D. Adware

3 **3. O que representa o spyware?**

- A. Software malicioso concebido para monitorizar secretamente as teclas premidas e as atividades do navegador
- B. Código de programa executado dentro de um contentor virtual em sandbox
- C. Atualizações anti-malware transferidas de registos de bases de dados
- D. Ajuste automático do brilho do ecrã

4 **4. Porque é que os programadores de malware usam rootkits?**

- A. Ocultar processos ativos e ficheiros maliciosos do sistema operativo
- B. Aumentar a velocidade de processamento do CPU nos endpoints
- C. Para fazer cópias de segurança de ficheiros de bases de dados em cofres seguros na nuvem
- D. Para melhorar a duração da bateria dos portáteis

5 **5. O que significa sandboxing na análise de malware?**

- A. Executar ficheiros suspeitos num cofre virtual isolado para observar o comportamento em segurança
- B. Analisar hashes de ficheiros em bases de dados de ameaças conhecidas
- C. Restaurar cópias de segurança de bases de dados após uma intrusão
- D. Desligar routers de rede local das linhas públicas

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. Os worms informáticos requerem a interação de um utilizador humano para se propagarem pelas redes locais.

- ◯ Verdadeiro
- ◯ Falso

7 Pergunta 7

7. O adware é sempre inofensivo e não rastreia o comportamento do utilizador nem o historial do navegador.

- ◯ Verdadeiro
- ◯ Falso

8 Pergunta 8

8. Restaurar cópias de segurança limpas e offline permite às vítimas recuperar ficheiros encriptados sem pagar o resgate.

- ◯ Verdadeiro
- ◯ Falso

9 Pergunta 9

9. O antivírus baseado em assinaturas impede de forma fiável o malware de dia zero antes de existir qualquer assinatura para ele.

- ◯ Verdadeiro
- ◯ Falso

10 Pergunta 10

10. O malware sem ficheiros executa scripts maliciosos na memória do sistema, evitando gravar ficheiros no disco.

- ◯ Verdadeiro
- ◯ Falso

Ponto de controlo 3: Inserção de termos-chave

Lê cada frase abaixo e preenche o espaço em branco com o termo correto do banco de palavras.

1. O malware disfarçado de programa utilitário seguro é um _____ .

2. As cargas maliciosas que bloqueiam sistemas de bases de dados a troco de dinheiro representam _____ .

3. Os keyloggers que registam palavras-passe em segredo representam _____ .

4. Esconder-se nas profundezas dos kernels dos sistemas operativos exige um _____ .

5. Analisar ficheiros suspeitos num cofre isolado recorre a uma _____ virtual.

6. Travar a propagação de cargas de malware ativas exige _____ imediata da rede.

BANCO DE PALAVRAS DE VOCABULÁRIO

CONTENÇÃO | RANSOMWARE | ROOTKIT | SANDBOX | SEM FICHEIROS | SPYWARE | TROIANO | VERME

Escreve aqui as tuas respostas:

1.
2.
3.
4.
5.
6.

Ponto de controlo 4: Associação de conceitos de segurança

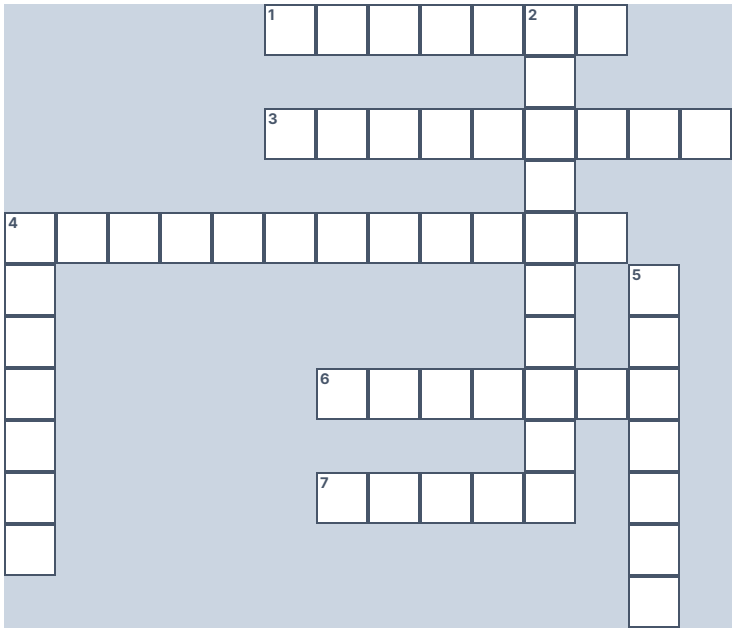
ASSOCIAÇÃO DE DEFINIÇÕES

Associa cada termo de vocabulário da esquerda à sua definição correta da direita, escrevendo a letra correspondente (A-H) na caixa de preenchimento.

☐	1. CAVALO DE TROIA	A	Programa concebido para monitorizar e registar secretamente a atividade e as introduções do utilizador.
☐	2. RANSOMWARE	B	Software malicioso executado diretamente na RAM para evitar a deteção por analisadores de disco.
☐	3. SPYWARE	C	Restringir os pontos finais infetados para impedir a propagação das cargas maliciosas.
☐	4. ROOTKIT	D	Software malicioso disfarçado de programa utilitário benigno ou útil.
☐	5. SANDBOX	E	Software malicioso autorreplicável que se propaga pelas redes sem ação humana.
☐	6. CONTENÇÃO	F	Software malicioso que encripta o armazenamento do sistema e exige pagamento para entregar a chave.
☐	7. WORM	G	Ambiente virtual isolado usado para analisar ficheiros maliciosos em segurança.
☐	8. SEM FICHEIROS	H	Software malicioso furtivo que se esconde no fundo dos kernels do sistema para manter o controlo administrativo.

Ponto de controlo 5: Palavras cruzadas

Resolve as palavras cruzadas escrevendo letras nas caixas brancas ativas. Os números correspondem às pistas abaixo.



HORIZONTAIS

1. Programa concebido para monitorizar e registar em segredo a atividade e as entradas do utilizador. (7)

3. Restringir os terminais infetados para evitar a propagação das cargas da ameaça. (9)

4. Malware que é executado diretamente na RAM para evitar a deteção por analisadores de disco. (12)

6. Software malicioso disfarçado de programa utilitário benigno ou útil. (7)

7. Malware autorreplicante que se propaga pelas redes sem intervenção humana. (5)

VERTICAIS

2. Malware que encripta o armazenamento do sistema e exige pagamento para entregar a chave. (10)

4. Ambiente virtual isolado usado para analisar ficheiros maliciosos em segurança. (7)

5. Malware furtivo escondido nas profundezas do kernel do sistema para manter o controlo administrativo. (7)

Ponto de controlo 5, alternativa: Pistas acessíveis das palavras cruzadas

Os utilizadores de leitores de ecrã e de teclado podem escrever as respostas das palavras cruzadas diretamente nos campos de texto abaixo.

HORIZONTAIS

1 horizontal: Programa concebido para monitorizar e registar em segredo a atividade e as entradas do utilizador. (7 letras):

3 horizontal: Restringir os terminais infetados para evitar a propagação das cargas da ameaça. (9 letras):

4 horizontal: Malware que é executado diretamente na RAM para evitar a deteção por analisadores de disco. (12 letras):

6 horizontal: Software malicioso disfarçado de programa utilitário benigno ou útil. (7 letras):

7 horizontal: Malware autorreplicante que se propaga pelas redes sem intervenção humana. (5 letras):

VERTICAIS

2 vertical: Malware que encripta o armazenamento do sistema e exige pagamento para entregar a chave. (10 letras):

4 vertical: Ambiente virtual isolado usado para analisar ficheiros maliciosos em segurança. (7 letras):

5 vertical: Malware furtivo escondido nas profundezas do kernel do sistema para manter o controlo administrativo. (7 letras):

Ponto de controlo 6: Sopa de letras

Encontra os 8 termos-chave de vocabulário escondidos na grelha abaixo. As palavras podem estar na horizontal, na vertical ou na diagonal.

V E R M E C P S O X L K Y K X
T K D Q M J D P N I R N N K Q
E X P G M M Q Y A R O S T T G
R O C S Q O H W I S O B W D S
A B Z V C Z W A O F T K H C Z
W D D N D Q X R R P K C U O B
M N A Z N D K E T A I D O N D
O A F H I D R Q M E T I R T Z
S S S F Q V F A A Q O N P E T
N X Q K R U S D N Y B F S N X
A S E M F I C H E I R O S C W
R J A R Z Y Y L G I M R J A M
L T O H Q Q H Z A O V G U O B
Y R Y B H L Z G J O P N W C M
Z Y G Y O W U K V P B N V T M

LISTA DE PALAVRAS DE VOCABULÁRIO

TROIANO RANSOMWARE SPYWARE ROOTKIT SANDBOX CONTENCAO VERME SEMFICHEIROS

Ponto de controlo 6, alternativa: Associação acessível de vocabulário

Associa cada um dos 8 termos de vocabulário da sopa de letras à sua definição correta, escrevendo a letra (A-H) no espaço em branco.

TERMOS DE VOCABULÁRIO

- **A. TROIANO**
- **B. RANSOMWARE**
- **C. SPYWARE**
- **D. ROOTKIT**
- **E. SANDBOX**
- **F. CONTENCAO**
- **G. VERME**
- **H. SEMFICHEIROS**

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO

1. Malware furtivo escondido nas profundezas do kernel do sistema para manter o controlo administrativo.
2. Restringir os terminais infetados para evitar a propagação das cargas da ameaça.
3. Malware que é executado diretamente na RAM para evitar a deteção por analisadores de disco.
4. Malware autorreplicante que se propaga pelas redes sem intervenção humana.
5. Malware que encripta o armazenamento do sistema e exige pagamento para entregar a chave.
6. Programa concebido para monitorizar e registar em segredo a atividade e as entradas do utilizador.
7. Software malicioso disfarçado de programa utilitário benigno ou útil.
8. Ambiente virtual isolado usado para analisar ficheiros maliciosos em segurança.

Ponto de controlo 7: Desafio de palavras baralhadas

Desembaralha as letras abaixo para revelar conceitos e termos essenciais de cibersegurança. Escreve as tuas respostas nas caixas de resposta fornecidas.

1. INTAOOR
2. SYERAWP
3. DSBXNOA
4. REMVE
5. AMEASWORRN
6. IOKRTTO
7. NCAOCTOEN
8. EMIRHSSCEOIF

Atividade bónus: Pensa rápido

3 RESPOSTAS POR CATEGORIA. GANHA QUEM COMPLETAR PRIMEIRO A LISTA.

1	Locais para transferir aplicações seguras			
2	Dispositivos que podem ser hackeados			
3	Coisas de que fazes cópia de segurança			
4	Sinais de alerta num email			
5	Sinais de que um telemóvel tem malware			
6	Tipos de malware que conheces			
7	Tipos de ficheiro com que ter cuidado			
8	Formas como o malware chega a um PC			
9	Hábitos seguros que podes começar hoje			
10	Palavras relacionadas com cibersegurança			
11	Coisas a fazer depois de uma fuga de dados			
12	Razões para atualizar o software			
13	Animais ou personagens com nomes parecidos com malware			
14	Coisas que o malware pode roubar			
15	Coisas a fazer se clicaste na ligação errada			

Ponto de controlo 8: Estudos de caso de cibersegurança

Aplica os conceitos que aprendeste para resolver os cenários reais abaixo.

ESTUDO DE CASO 1: CONTENÇÃO DE CARGA DE RANSOMWARE EMPRESARIAL



Cenário: Uma rede local empresarial foi comprometida por ransomware ativo. Os servidores de ficheiros principais começaram a mostrar ficheiros com a extensão .locked. Estabelece políticas de contenção.

Questão para debate: Detalha os passos de contenção e descreve o protocolo de recuperação de dados.

ESTUDO DE CASO 2: INJEÇÃO NA MEMÓRIA POR MALWARE SEM FICHEIROS



Cenário: Um analista deteta padrões de scripting suspeitos a serem executados diretamente na RAM volátil do sistema com ferramentas administrativas normais, mas não existem ficheiros maliciosos no disco.

Questão para debate: Explica a estratégia de análise de memória e indica ferramentas para bloquear a execução sem ficheiros.

Ponto de controlo 9: Decifrar o código

Um profissional de cibersegurança protege os ativos de rede contra agentes de ameaça online. Usa a chave Letra-Número abaixo para decifrar a mensagem, escrevendo as letras correspondentes nos espaços em branco.

CHAVE DE ENCRIPTAÇÃO DE LETRAS PARA NÚMEROS

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

4 5 20 5 20 1 1 13 5 1 3 1 19 3 15 13

13 15 14 9 20 15 18 9 26 1 3 1 15

3 15 13 16 15 18 20 1 13 5 14 20 1 12

Mensagem decifrada:

DICA: CADA NÚMERO REPRESENTA A POSIÇÃO DESSA LETRA NO ALFABETO (P. EX., 1 = A, 2 = B, 26 = Z).

Ponto de controlo 10: Perguntas frequentes básicas sobre cibersegurança (Parte A)

Revê perguntas e respostas comuns sobre a mitigação de ameaças online.

Q1: O que é malware?

Software malicioso criado por agentes de ameaças para danificar, sequestrar ou roubar dados de dispositivos e redes.

Q2: Qual é a diferença entre um vírus e um worm?

Um vírus precisa de uma ação humana (como abrir um ficheiro) para se propagar, ao passo que um worm propaga-se automaticamente pelas redes.

Q3: Como infeta um cavalo de Troia um computador?

Engana os utilizadores fazendo-se passar por um programa inofensivo ou seguro, escondendo lá dentro a sua carga maliciosa.

Q4: O que é o ransomware?

Um tipo de software malicioso que encripta os ficheiros do sistema alvo e exige um pagamento financeiro em troca da chave de desencriptação. [1]

Q5: O que é o spyware?

Software malicioso que regista em segredo as teclas premidas, as palavras-passe e os hábitos de navegação do utilizador para os enviar aos atacantes.

Ponto de controlo 10: Perguntas frequentes básicas sobre cibersegurança (Parte B)

Revê perguntas e respostas comuns sobre a mitigação de ameaças online.

Q6: O que significa sandboxing?

Executar ficheiros suspeitos num ambiente virtual seguro e isolado para observar o seu comportamento sem risco para os sistemas de produção.

Q7: O que é o malware sem ficheiros (fileless)?

Software malicioso que é executado diretamente na memória do sistema (RAM) através de utilitários legítimos, evitando gravar ficheiros no disco para contornar os analisadores básicos.

Q8: Como protege um rootkit o malware?

Esconde processos e ficheiros maliciosos, muitas vezes subvertendo o kernel do sistema operativo, pelo que os scanners de antivírus podem não os detetar.

Q9: O que é a monitorização dinâmica de comportamento?

Análise antivírus que monitoriza processos ativos em tempo real para bloquear ações típicas de software malicioso, como a encriptação em massa de ficheiros.

Q10: Porque é urgente a contenção durante a resposta a incidentes?

Isolar os dispositivos terminais comprometidos impede que cargas ativas de software malicioso se propaguem a outros dispositivos de rede.

Ponto de controlo 10: Perguntas frequentes avançadas sobre segurança (Parte C)

Explora aspetos técnicos avançados das estruturas de segurança, da análise de malware e da conformidade de dados.

Q1: Como é que os criadores de malware contornam os antivírus baseados em assinaturas?

Usam polimorfismo, alterando o hash e a estrutura de código do ficheiro a cada infeção, mantendo o mesmo comportamento malicioso.

Q2: Qual é o risco das ferramentas de dupla utilização em campanhas de malware?

Os atacantes usam ferramentas administrativas legítimas (como o PowerShell ou o Sysinternals) para se misturarem com o tráfego de rede normal, dificultando a deteção.

Q3: Como executa o process hollowing cargas maliciosas?

Lança um processo legítimo do sistema num estado suspenso, substitui o seu código em memória por software malicioso e retoma a execução.

Q4: Qual é o papel de um servidor de comando e controlo (C2)?

Um servidor remoto operado por hackers para enviar instruções e cargas a software malicioso em execução em máquinas comprometidas.

Q5: Porque é difícil detetar o keylogging?

Os keyloggers básicos consomem recursos mínimos de CPU e escondem os seus processos dentro de utilitários legítimos do espaço do utilizador.

Ponto de controlo 10: Perguntas frequentes avançadas sobre segurança (Parte D)

Explora aspetos técnicos avançados das estruturas de segurança, da análise de malware e da conformidade de dados.

Q6: Como atrasa a ofuscação de código a análise de malware?

Encripta ou reorganiza o código-fonte, tornando-o ilegível para as ferramentas de análise e os scanners de segurança.

Q7: Qual é a função de um bootkit?

Um rootkit que infeta o processo de arranque (o MBR, o setor de arranque ou o firmware UEFI), pelo que é executado antes de o sistema operativo carregar.

Q8: Como identifica a análise heurística ameaças de dia zero?

Procura padrões de código suspeitos e comandos administrativos em vez de procurar um hash correspondente numa base de dados.

Q9: Qual é a ameaça do sequestro de DLL?

Forçar uma aplicação legítima a carregar uma biblioteca de ligação dinâmica (DLL) maliciosa, colocando-a no caminho do diretório da aplicação.

Q10: Como é que os pipelines automatizados de análise de malware usam a virtualização?

Executam ficheiros suspeitos em várias VMs de sistemas operativos, gerando automaticamente registos de comportamento e ficheiros PCAP de rede.

Parte 11: 10 factos e perspetivas do mundo real sobre cibersegurança

Revê factos reais sobre violações de segurança, mecanismos de defesa e normas de conformidade.

1. PERSPETIVA SOBRE SEGURANÇA

Os cavalos de Troia continuam a ser um método de infeção comum porque escondem código malicioso dentro de programas que parecem inofensivos.

2. PERSPETIVA SOBRE SEGURANÇA

O IC3 do FBI recebeu mais de 3600 queixas de ransomware em 2025, com perdas comunicadas superiores a 32 milhões de dólares. [3]

3. PERSPETIVA SOBRE SEGURANÇA

Os worms podem propagar-se rapidamente pelas redes ao explorar vulnerabilidades de protocolo não corrigidas, como o EternalBlue no SMB.

4. PERSPETIVA SOBRE SEGURANÇA

O malware sem ficheiros é difícil de detetar porque corre na memória através de ferramentas legítimas e deixa poucos vestígios no disco.

5. PERSPETIVA SOBRE SEGURANÇA

As sandboxes de análise normalmente regressam a um instantâneo limpo após cada execução, para que cada teste comece de um estado conhecido.

6. PERSPETIVA SOBRE SEGURANÇA

Os rootkits podem modificar as chamadas de sistema do kernel, comunicando resultados de diagnóstico falsos aos analisadores de software malicioso.

7. PERSPETIVA SOBRE SEGURANÇA

A ofuscação de código utiliza utilitários de empacotamento para comprimir e ocultar a verdadeira estrutura da carga binária do malware.

8. PERSPETIVA SOBRE SEGURANÇA

O malware polimórfico altera o seu código, e por isso o seu hash de ficheiro, a cada nova cópia para evitar as verificações de assinaturas.

9. PERSPETIVA SOBRE SEGURANÇA

O sequestro de DLL explora as configurações da ordem de pesquisa em sistemas operativos comuns, como o Windows.

10. PERSPETIVA SOBRE SEGURANÇA

Os fornecedores de segurança encontram diariamente um enorme número de novas amostras de software malicioso, pelo que as assinaturas precisam de atualizações constantes.

Referências técnicas e fontes

O guia de estudo e os puzzles interativos são compilados a partir das normas globais do NIST, da OWASP e de conformidade em matéria de privacidade de dados.

REFERÊNCIAS ACADÉMICAS E DO SETOR

[1] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Soluções: Ponto de controlo 1 - Escolha múltipla

1 Pergunta 1

Resposta correta: A

NOTA PARA O PROFESSOR

Qual é a característica definidora de um cavalo de Troia? → Disfarça-se de software legítimo para enganar os utilizadores e levá-los a executá-lo

2 Pergunta 2

Resposta correta: A

NOTA PARA O PROFESSOR

Que tipo de malware encripta ficheiros e exige pagamento? → Ransomware [1]

3 Pergunta 3

Resposta correta: A

NOTA PARA O PROFESSOR

O que representa o spyware? → Software malicioso concebido para monitorizar secretamente as teclas premidas e as atividades do navegador

4 Pergunta 4

Resposta correta: A

NOTA PARA O PROFESSOR

Porque é que os programadores de malware usam rootkits? → Ocultar processos ativos e ficheiros maliciosos do sistema operativo

5 Pergunta 5

Resposta correta: A

NOTA PARA O PROFESSOR

O que significa sandboxing na análise de malware? → Executar ficheiros suspeitos num cofre virtual isolado para observar o comportamento em segurança

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 Pergunta 6

Resposta correta: Falso

NOTA PARA O PROFESSOR

Falso: os worms replicam-se sozinhos e espalham-se pelas redes sem qualquer ação do utilizador.

7 Pergunta 7

Resposta correta: Falso

NOTA PARA O PROFESSOR

Falso: o adware nem sempre é inofensivo; grande parte monitoriza a navegação para direcionar anúncios.

8 Pergunta 8

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

Verdadeiro: cópias de segurança offline limpas restauram os ficheiros encriptados sem pagar, embora os dados roubados ainda possam ser divulgados.

9 Pergunta 9

Resposta correta: Falso

NOTA PARA O PROFESSOR

Falso: os analisadores de assinaturas precisam de uma amostra conhecida, pelo que o malware de dia zero totalmente novo pode passar despercebido.

10 Pergunta 10

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

O malware sem ficheiros executa scripts maliciosos na memória do sistema, evitando gravar ficheiros no disco.

Soluções de vocabulário e grelha de avaliação

Grelha de classificação do professor: atribui 1 ponto por cada correspondência correta (8 pontos no total) e por cada termo de contexto (6 pontos no total).

PONTO DE CONTROLO 4: SOLUÇÕES – ASSOCIAÇÃO DE CONCEITOS

D 1. CAVALO DE TROIA	F 2. RANSOMWARE	A 3. SPYWARE	H 4. ROOTKIT
G 5. SANDBOX	C 6. CONTENÇÃO	E 7. WORM	B 8. SEM FICHEIROS

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 TROIANO	2 RANSOMWARE	3 SPYWARE	4 ROOTKIT
5 SANDBOX	6 CONTENÇÃO		

PONTO DE CONTROLO 6, ALTERNATIVA: SOLUÇÕES – ASSOCIAÇÃO DE PALAVRAS

1 D – ROOTKIT	2 F – CONTENCAO	3 H – SEMFICHEIROS	4 G – VERME
5 B – RANSOMWARE	6 C – SPYWARE	7 A – TROIANO	8 E – SANDBOX

NOTAS DE DEBATE PARA PROFESSORES

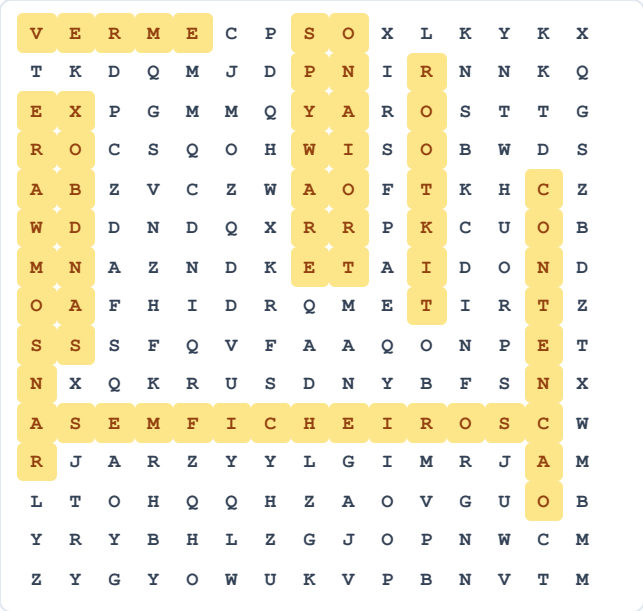
Termos-chave:
Verifica se os alunos sabem explicar CAVALO DE TROIA, RANSOMWARE e SPYWARE por palavras suas e dar um exemplo de cada.

Estudos de caso:
Pede aos alunos que justifiquem as recomendações com factos da ficha e não com suposições.

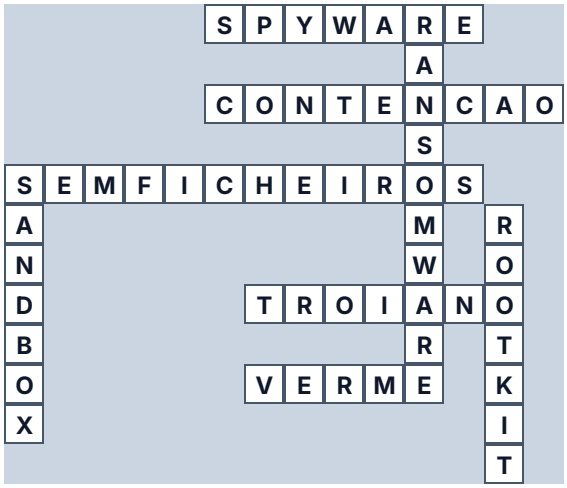
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS



SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

1 horizontal: SPYWARE Programa concebido para monitorizar e registar em segredo a atividade e as entradas do utilizador. (7 letras)

3 horizontal: CONTENCAO Restringir os terminais infetados para evitar a propagação das cargas da ameaça. (9 letras)

4 horizontal: SEMFICHEIROS Malware que é executado diretamente na RAM para evitar a deteção por analisadores de disco. (12 letras)

6 horizontal: TROIANO Software malicioso disfarçado de programa utilitário benigno ou útil. (7 letras)

7 horizontal: VERME Malware autorreplicante que se propaga pelas redes sem intervenção humana. (5 letras)

VERTICAIS

2 vertical: RANSOMWARE Malware que encripta o armazenamento do sistema e exige pagamento para entregar a chave. (10 letras)

4 vertical: SANDBOX Ambiente virtual isolado usado para analisar ficheiros maliciosos em segurança. (7 letras)

5 vertical: ROOTKIT Malware furtivo escondido nas profundezas do kernel do sistema para manter o controlo administrativo. (7 letras)

Palavras baralhadas e soluções da cifra

Chave de correção da atividade de reordenação de letras do vocabulário e do Desafio do Código Secreto.

CHAVE DE SOLUÇÕES DAS PALAVRAS EMBARALHADAS

1. INTAOOR — **TROIANO**
2. SYERAWP — **SPYWARE**
3. DSBXNOA — **SANDBOX**
4. REMVE — **VERME**
5. AMEASWORRN — **RANSOMWARE**
6. IOKRTTO — **ROOTKIT**
7. NCAOCTOEN — **CONTENCAO**
8. EMIRHSSCEOIF — **SEMFICHEIROS**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"DETETA AMEACAS COM MONITORIZACAO COMPORTAMENTAL"

Soluções dos estudos de caso

A Estudo de caso 1: Contenção de carga de ransomware empresarial

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: A rede local de uma empresa foi violada por ransomware ativo. Os principais servidores de ficheiros começaram a mostrar ficheiros com a extensão .locked. Estabelece políticas de contenção.
- Estratégia e solução recomendadas: Desligar da rede local todos os servidores afetados. Terminar as sessões administrativas ativas. Restaurar os ficheiros não comprometidos a partir de um sistema de cópia de segurança offline seguro, com proteção contra escrita.

B Estudo de caso 2: Injeção na memória por malware sem ficheiros

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Um analista deteta padrões de scripting suspeitos a executar-se diretamente na RAM volátil do sistema com ferramentas administrativas padrão, mas não existem ficheiros maliciosos no disco.
- Estratégia e solução recomendadas: Isolar os pontos finais afetados e capturar primeiro uma imagem da memória. Rever os registos de PowerShell e WMI, bloquear scripts não aprovados com o AppLocker e depois reiniciar para eliminar a carga maliciosa.