名前: 日付: 得点:

マルウェア分析と脅威の軽減ガイド

トロイの木馬、ランサムウェア、スパイウェア、ルートキット、仮想化サンドボックス、封じ込め

マルウェア分析 学習概要

保護済み
データ暗号化
256 ビット AES 標準

準拠
世界標準
GDPR と CCPA の枠組み

ゼロトラスト
アクセスポリシー
多要素認証

ようこそ！ このアクティビティ資料では、マルウェアの分析と防止について学びます。スパイウェア、トロイの木馬、ランサムウェアのペイロード、リバースエンジニアリングツール、ルートキットの挙動、封じ込めの戦略を取り上げます。

ワークシートのチェックポイント

- [ ] パート 1-4: サイバーセキュリティと脅威の防止を習得します。
- [ ] パート 5-7: クロスワードと単語探しのパズルを解きます。
- [ ] パート 8-9: ケーススタディと暗号チャレンジを解きます。
- [ ] パート 10: 基礎と応用の FAQ ページを確認します。
- [ ] パート 11: 実世界の興味深い事実10選を調べます。
- [ ] ボーナス: すばやく考えよう チャレンジ

VPN.com のサイバーセキュリティガイドを開く

URL: https://www.vpn.com/cybersecurity/malware/

あなたのマルウェア対策 学習ロードマップ

- トロイの木馬、ワーム、ルートキットというマルウェアの種類の違いを説明します。
- コード分析のために、サンドボックス仮想化による実行を導入する。
- 活動中のランサムウェアのペイロードに対する、封じ込めと無害化の計画を設計します。

マルウェア分析ガイド 手順

多肢選択問題と正誤問題に答え、語群を使って穴埋め文を完成させ、定義を結び付け、クロスワードと単語探しパズルを解いてください。学んだ知識をマルウェアの被害軽減に応用しましょう。 最後にボーナス活動「すばやく考えよう」に取り組みましょう。

マルウェア分析と脅威の封じ込め（入門）

トロイの木馬、ワーム、ランサムウェアなどの悪意あるコードは、エンドポイントやサーバーに大きな影響を与える脅威です。セキュリティチームは仮想サンドボックス内でマルウェアを分析し、ペイロードの拡散を抑えるために迅速にネットワークを隔離します。

各チェックポイントをよく読んで、正しいものを選ぶか書いてください。

チェックポイント 1: 多肢選択チャレンジ

1. 1. トロイの木馬を特徴づけるものは何ですか?
   - A. 正規のソフトウェアを装い、ユーザーをだまして実行させる
   - B. ローカルネットワーク回線を通じて自動的に複製される
   - C. 隔離された仮想サンドボックス内のファイルに感染する
   - D. インターネットサービスプロバイダーのトラフィックを傍受する

2. 2. ファイルを暗号化して支払いを要求するマルウェアの種類はどれですか?
   - A. ランサムウェア
   - B. スパイウェア
   - C. ルートキット
   - D. アドウェア

3. 3. スパイウェアに当たるものは何ですか?
   - A. ユーザーのキー入力とブラウザーでの操作をひそかに監視するよう設計されたマルウェア
   - B. サンドボックス化された仮想コンテナ内で実行されるプログラムコード
   - C. データベースレジストリからダウンロードされるマルウェア対策の更新
   - D. 画面の明るさの自動調整

4. 4. マルウェアの開発者がルートキットを使うのはなぜですか?
   - A. 実行中のプロセスや悪意のあるファイルをOSから隠すため
   - B. エンドポイントでのCPU処理速度を上げるため
   - C. データベースファイルを安全なクラウド保管庫にバックアップするため
   - D. ノートパソコンのバッテリー持ちを改善するため

5. 5. マルウェア分析で、サンドボックス化とはどういう意味ですか?
   - A. 隔離された仮想の保管庫で不審なファイルを実行し、動作を安全に観察する
   - B. ファイルのハッシュを既知の脅威データベースと照合してスキャンすること
   - C. 侵入後にデータベースのバックアップを復元すること
   - D. ローカルネットワークのルーターを公衆回線から切断すること

チェックポイント 2: 正しい・誤りチャレンジ

6 質問 6

6. コンピューターワームがローカルネットワーク上で拡散するには、ユーザーの操作が必要である。

○ 正しい ○ 誤り

7 質問 7

7. アドウェアは常に無害で、ユーザーの行動やブラウザーの履歴を追跡しません。

○ 正しい ○ 誤り

8 質問 8

8. クリーンなオフラインバックアップを復元すれば、被害者は身代金を支払わなくても暗号化されたファイルを回復できます。

○ 正しい ○ 誤り

9 質問 9

9. シグネチャ型のアンチウイルスは、シグネチャが存在する前のゼロデイのマルウェアを確実に阻止します。

○ 正しい ○ 誤り

10 質問 10

10. ファイルレスマルウェアは、ディスクにファイルを書き込まず、システムメモリ内で悪意のあるスクリプトを実行します。

○ 正しい ○ 誤り

チェックポイント 3: 重要用語の穴埋め

以下の各文を読み、空欄にワードバンクから正しい用語を入れてください。

1. 安全なユーティリティプログラムに偽装したマルウェアは _____ です。
2. お金目的でデータベースシステムをロックする悪意あるペイロードは _____ です。
3. パスワードを密かに記録するキーロガーは _____ の一種です。
4. オペレーティングシステムのカーネルの奥深くに潜むには、 _____ が必要です。
5. 疑わしいファイルを隔離された金庫で解析するには、仮想の _____ を使います。
6. 稼働中のマルウェアのペイロードの拡散を止めるには、ネットワークの即時 _____ が必要です。

用語バンク

サンドボックス　スパイウェア　トロイの木馬　ファイルレス　ランサムウェア
ルートキット　ワーム　封じ込め

ここに答えを書いてください:

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

チェックポイント 4: セキュリティの概念マッチング

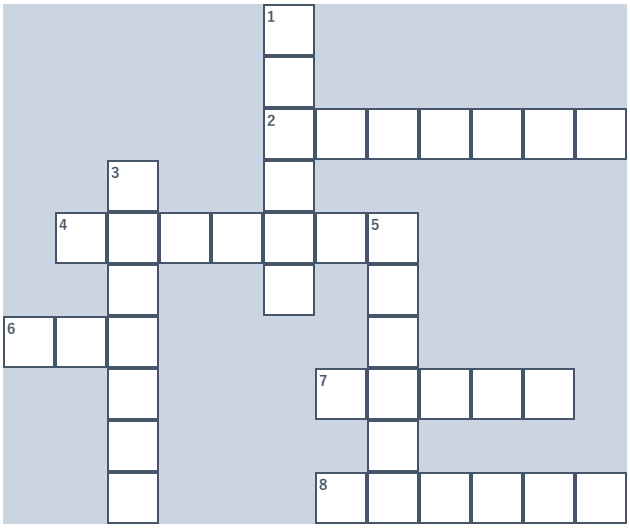
定義マッチング

左の各用語を、入力欄に対応する文字（A〜H）を入力して、右の正しい定義と組み合わせてください。

1. トロイの木馬	A	ユーザーの操作や入力を密かに監視して記録するよう設計されたプログラム。
2. ランサムウェア	B	基本的なスキャナーに検出されないよう、RAM 上で直接実行されるマルウェア。
3. スパイウェア	C	脅威のペイロードの拡散を防ぐために、感染したエンドポイントを制限すること。
4. ルートキット	D	無害または便利なユーティリティプログラムを装った悪意のあるソフトウェア。
5. サンドボックス	E	人の操作なしにネットワーク間で自己複製して広がるマルウェア。
6. 封じ込め	F	システムのストレージを暗号化し、鍵の引き渡しと引き換えに支払いを要求するマルウェア。
7. ワーム	G	悪意のあるファイルを安全に分析するために使われる、隔離された仮想環境。
8. ファイルレス	H	システムカーネルの奥深くに潜み、管理者権限の制御を維持するステルス型マルウェア。

チェックポイント 5: クロスワードパズル

有効な白いマスに文字を入力して、クロスワードパズルを解いてください。数字は下のカギに対応しています。



ヨコのカギ

2. 無害または便利なユーティリティプログラムに見せかけた悪意のあるソフトウェア (7)

4. 悪意のあるファイルを安全に解析するための隔離された仮想環境 (7)

6. 人の操作なしにネットワーク上で広がる、自己複製型のマルウェア (3)

7. 脅威のペイロードが広がらないよう、感染した端末を制限すること (5)

8. ディスクスキャナーによる検出を避けるため、RAM上で直接実行されるマルウェア (6)

タテのカギ

1. システムのカーネルの奥深くに潜み、管理者権限を維持し続ける隠蔽型マルウェア (6)

3. システムのストレージを暗号化し、鍵の引き渡しと引き換えに金銭を要求するマルウェア (7)

5. ユーザーの操作や入力を密かに監視して記録するよう作られたプログラム (6)

チェックポイント 5 代替活動: アクセシブルなクロスワードのヒント

スクリーンリーダーやキーボードを使うユーザーは、下の入力欄にクロスワードの答えを直接入力できます。

ヨコのカギ

2 ヨコ: 無害または便利なユーティリティプログラムに見せかけた悪意のあるソフトウェア (7 文字):

4 ヨコ: 悪意のあるファイルを安全に解析するための隔離された仮想環境 (7 文字):

6 ヨコ: 人の操作なしにネットワーク上で広がる、自己複製型のマルウェア (3 文字):

7 ヨコ: 脅威のペイロードが広がらないよう、感染した端末を制限すること (5 文字):

8 ヨコ: ディスクスキャナーによる検出を避けるため、RAM上で直接実行されるマルウェア (6 文字):

タテのカギ

1 タテ: システムのカーネルの奥深くに潜み、管理者権限を維持し続ける隠蔽型マルウェア (6 文字):

3 タテ: システムのストレージを暗号化し、鍵の引き渡しと引き換えに金銭を要求するマルウェア (7 文字):

5 タテ: ユーザーの操作や入力を密かに監視して記録するよう作られたプログラム (6 文字):

チェックポイント 6: 隠れた単語さがし

下のグリッドに隠れている8つの重要な用語を見つけてください。単語は横、縦、斜めに並んでいます。

ペ ロ ボ タ レ ミ ク グ ヌ チ ユ ガ メ ロ ボ
ワ ラ メ キ ゼ ゴ ザ ス ス ホ フ ノ オ ア オ
キ ル コ パ ホ ヒ パ ヘ ボ パ ア ズ フ サ ン
メ ハ ジ ト ツ キ ト ー ル コ イ ヌ ヤ モ ヘ
ワ レ ウ テ モ ト モ ン ギ ゲ ル ウ ズ ジ ツ
ス カ フ ゴ ワ ロ ラ ラ ニ グ レ カ エ バ コ
ク ザ ペ ダ キ イ ポ バ ン タ ス フ ト ア ー
ツ コ モ サ ガ ノ ベ レ カ サ ゾ エ ア ー ユ
ボ コ ヘ イ サ モ ラ サ ソ テ ム ヌ コ ギ ン
ド メ ス ヌ グ ク ポ ゴ ソ ガ ド ウ セ イ イ
ン ガ リ ヤ レ バ ズ ボ ワ ヒ グ ゼ エ ゲ ケ
サ ヤ プ オ タ グ ベ ブ ノ ム イ ギ ー ア ピ
ピ マ ツ ヌ メ ガ ヒ ム ー ミ ジ リ ト ロ ン
テ ー ウ ラ デ チ ダ ワ カ プ グ プ オ ト ミ
ー ツ ハ ヨ レ ユ ブ キ ム ー プ チ ピ リ ビ

用語リスト

トロイノモクバ　ランサムウエア　スパイウエア　ルートキツト　サンドボツクス
フウジコメ　ワーム　フアイルレス

チェックポイント 6 代替活動: アクセシブルな用語マッチング

ワードサーチの 8 つの用語を、空欄に文字（A〜H）を書いて、正しい定義と組み合わせてください。

用語
A. トロイノモクバ
B. ランサムウエア
C. スパイウエア
D. ルートキツト
E. サンドボツクス
F. フウジコメ
G. ワーム
H. フアイルレス

定義とマッチ欄
1. システムのカーネルの奥深くに潜み、管理者権限を維持し続ける隠蔽型マルウェア。
2. 脅威のペイロードが広がらないよう、感染した端末を制限すること。
3. ディスクスキャナーによる検出を避けるため、RAM上で直接実行されるマルウェア。
4. 人の操作なしにネットワーク上で広がる、自己複製型のマルウェア。
5. システムのストレージを暗号化し、鍵の引き渡しと引き換えに金銭を要求するマルウェア。
6. ユーザーの操作や入力を密かに監視して記録するよう作られたプログラム。
7. 無害または便利なユーティリティプログラムに見せかけた悪意のあるソフトウェア。
8. 悪意のあるファイルを安全に解析するための隔離された仮想環境。

チェックポイント 7: 並べ替え単語チャレンジ

下の文字を並べ替えて、サイバーセキュリティの重要な概念と用語を見つけましょう。答えは用意された入力欄に書いてください。

1. ノクトモバイロ
2. アスイエウパ
3. ボサツスドクン
4. ームワ
5. ウアムサラエン
6. ツキルトトー
7. コメフジウ
8. イスフレルア

ボーナス活動: すばやく考えよう

それぞれのカテゴリーで答えを 3 つ書きましょう。最初にリストを埋めた人の勝ちです。

1	安全なアプリをダウンロードできる場所			
2	ハッキングされるおそれのあるデバイス			
3	バックアップするもの			
4	メールの危険なサイン			
5	スマートフォンがマルウェアに感染しているサイン			
6	知っているマルウェアの種類			
7	注意すべきファイルの種類			
8	マルウェアがPCに入り込む経路			
9	今日から始められる安全な習慣			
10	サイバーセキュリティに関連する言葉			
11	データが漏えいした後にすること			
12	ソフトウェアを更新する理由			
13	マルウェアのような名前を持つ動物やキャラクター			
14	マルウェアが盗めるもの			
15	間違ったリンクをクリックしたときにすること			

チェックポイント 8: サイバーセキュリティのケーススタディ

学んだ概念を応用して、以下の実際のシナリオを解いてみましょう。

ケーススタディ 1: 企業でのランサムウェアのペイロードの封じ込め



シナリオ: ある企業のローカルエリアネットワークが、活動中のランサムウェアに侵害されました。 主要なファイルサーバーで、ファイル拡張子が .locked と表示され始めています。封じ込めのポリシーを確立してください。

ディスカッションの問い: 封じ込めの手順を詳しく説明し、データ復旧のプロトコルを概説できますか？

ケーススタディ 2: ファイルレスマルウェアによるメモリインジェクション



シナリオ: アナリストが、標準的な管理ツールを使って揮発性のシステムRAM上で直接実行されている不審なスクリプトのパターンを検出しますが、ディスク上には悪意のあるファイルは存在しません。

ディスカッションの問い: メモリ分析の戦略を説明し、ファイルレス実行をブロックするツールを示せますか？

チェックポイント 9: 暗号を解読しよう

サイバーセキュリティの専門家は、ネットワーク資産をオンラインの脅威アクターから守ります。下の文字と数字の対応表を使い、対応する文字を空欄に書いて、メッセージを解読してください。

文字から数字への暗号鍵

ア=1 イ=2 ウ=3 エ=4 オ=5 カ=6 キ=7 ク=8 ケ=9 コ=10 サ=11 シ=12

ス=13 セ=14 ソ=15 タ=16 チ=17 ツ=18 テ=19 ト=20 ナ=21 ニ=22 ヌ=23 ネ=24

ノ=25 ハ=26 ヒ=27 フ=28 ヘ=29 ホ=30 マ=31 ミ=32 ム=33 メ=34 モ=35 ヤ=36

ユ=37 ヨ=38 ラ=39 リ=40 ル=41 レ=42 ロ=43 ワ=44 ヲ=45 ン=46 ガ=47 ギ=48

グ=49 ゲ=50 ゴ=51 ザ=52 ジ=53 ズ=54 ゼ=55 ゾ=56 ダ=57 ヂ=58 ヅ=59 デ=60

ド=61 バ=62 ビ=63 ブ=64 ベ=65 ボ=66 パ=67 ピ=68 プ=69 ペ=70 ポ=71 ー=72

16	46	31	18	25		28	41	31	2	45		6	46	12	12	19

9	46	17	13	41

解読したメッセージ:

ヒント: 各数字は、上の暗号鍵のカタカナ 1 文字を表します。

チェックポイント 10: サイバーセキュリティ FAQ – 基礎 (パート A)

オンラインの脅威への対策に関するよくある質問と回答を確認しましょう。

Q1: マルウェアとは何ですか?

脅威アクターが、デバイスやネットワークに損害を与えたり、乗っ取ったり、データを盗んだりするために作成した悪意のあるソフトウェア。

Q2: ウイルスとワームの違いは何ですか?

ウイルスが広がるには(ファイルを開くなど)人の操作が必要ですが、ワームはネットワーク間で自動的に広がります。

Q3: トロイの木馬はどのようにコンピューターに感染しますか?

無害で安全なプログラムを装ってユーザーをだまし、内部に悪意のあるペイロードを隠します。

Q4: ランサムウェアとは何ですか?

対象システム上のファイルを暗号化し、復号鍵と引き換えに金銭の支払いを要求するマルウェアの一種。 [1]

Q5: スパイウェアとは何ですか?

ユーザーのキー入力、パスワード、閲覧習慣をひそかに記録して攻撃者に送信する悪意のあるソフトウェア。

チェックポイント 10: サイバーセキュリティ FAQ – 基礎 (パート B)

オンラインの脅威への対策に関するよくある質問と回答を確認しましょう。

Q6: サンドボックス化とはどういう意味ですか?

本番システムにリスクを与えずに動作を観察するため、疑わしいファイルを安全で隔離された仮想環境で実行すること。

Q7: ファイルレスマルウェアとは何ですか?

正規のユーティリティを使ってシステムメモリ（RAM）上で直接動作し、基本的なスキャナーをすり抜けるためにディスクへのファイル書き込みを避けるマルウェア。

Q8: ルートキットはマルウェアをどう隠しますか?

悪意のあるプロセスやファイルを、多くの場合オペレーティングシステムのカーネルを乗っ取ることで隠すため、ウイルス対策スキャナーが見逃すことがあります。

Q9: 動的な動作監視とは何ですか?

実行中のプロセスをリアルタイムで監視し、ファイルの一括暗号化などマルウェア特有の動作をブロックする、ウイルス対策のスキャン。

Q10: なぜインシデント対応では封じ込めが急務なのですか?

侵害されたエンドポイントを隔離すると、動作中のマルウェアのペイロードが他のネットワークデバイスに広がるのを防げます。

チェックポイント 10: セキュリティ FAQ – 応用 (パート C)

セキュリティフレームワーク、マルウェア分析、データコンプライアンスについて、高度な技術的側面を探ります。

Q1: マルウェアの開発者は、シグネチャベースのウイルス対策スキャナーをどのように回避しますか?

ポリモーフィズムを利用し、悪意のある動作は同じままで、感染のたびにファイルのハッシュとコード構造を変更します。

Q2: マルウェアキャンペーンにおける二重用途ツールのリスクは何ですか?

攻撃者は、正規の管理ツール（PowerShellやSysinternalsなど）を使って通常のネットワークトラフィックに紛れ込み、検出を困難にします。

Q3: プロセスハロウィングは悪意のあるペイロードをどう実行しますか?

正規のシステムプロセスを停止状態で起動し、そのメモリー上のコードをマルウェアに置き換えて、実行を再開します。

Q4: コマンド&コントロール(C2)サーバーの役割は何ですか?

ハッカーが運用するリモートサーバーで、侵害されたマシン上で動くマルウェアに指示やペイロードを送ります。

Q5: キーロギングが検出しにくいのはなぜですか?

基本的なキーロガーはCPUリソースをほとんど消費せず、正規のユーザー空間ユーティリティの中にプロセスを隠します。

チェックポイント 10: セキュリティ FAQ – 応用 (パート D)

セキュリティフレームワーク、マルウェア分析、データコンプライアンスについて、高度な技術的側面を探ります。

Q6: コードの難読化はマルウェア分析をどう遅らせますか?

ソースコードを暗号化または並べ替えて、解析ツールやセキュリティスキャナーが読めないようにします。

Q7: ブートキットの機能は何ですか?

ブートプロセス(MBR、ブートセクター、UEFIファームウェア)に感染するルートキットで、OSが読み込まれる前に動作します。

Q8: ヒューリスティックスキャンはゼロデイの脅威をどう識別しますか?

データベースのハッシュとの一致を探すのではなく、疑わしいコードのパターンや管理者コマンドをスキャンします。

Q9: DLL ハイジャックの脅威とは何ですか?

アプリケーションのディレクトリパスに置くことで、正規のアプリケーションに悪意のあるダイナミックリンクライブラリ(DLL)を読み込ませること。

Q10: 自動化されたマルウェア分析パイプラインは、仮想化をどのように利用しますか?

不審なファイルを複数のOSの仮想マシンで実行し、動作ログとネットワークのPCAPファイルを自動で生成します。

パート 11: 実世界のサイバーセキュリティの事実10選と洞察

セキュリティ侵害、防御の仕組み、コンプライアンス基準に関する実際の事実を確認しましょう。

1. セキュリティの洞察

トロイの木馬は、無害に見えるプログラムの中に悪意のあるコードを隠すため、今でも一般的な感染手段です。

2. セキュリティの洞察

FBIのIC3は2025年に3,600件を超えるランサムウェアの被害届を受け、報告された損失額は3,200万ドルを超えました。[3]

3. セキュリティの洞察

ワームは、SMBのEternalBlueのように、修正されていないプロトコルの脆弱性を悪用して、ネットワーク上で急速に拡散する可能性があります。

4. セキュリティの洞察

ファイルレスマルウェアは、正規のツールを通じてメモリ内で動作し、ディスク上にほとんど痕跡を残さないため、検出が困難です。

5. セキュリティの洞察

分析用のサンドボックスは、通常、実行のたびにクリーンなスナップショットへ戻るため、すべてのテストが既知の状態から始まります。

6. セキュリティの洞察

ルートキットはカーネルのシステムコールを改ざんし、マルウェア対策スキャナーに偽の診断結果を報告することがあります。

7. セキュリティの豆知識

コードの難読化では、パッカーユーティリティを使って圧縮し、マルウェアの実際のバイナリペイロードの構造を隠します。

8. セキュリティの豆知識

ポリモーフィック型マルウェアは、シグネチャチェックを回避するため、新しいコピーのたびにコードを、したがってファイルのハッシュも変化させます。

9. セキュリティの豆知識

DLLハイジャックは、Windowsなどの標準的なオペレーティングシステムの検索順序の設定を悪用します。

10. セキュリティの洞察

セキュリティベンダーは毎日膨大な数の新しいマルウェアのサンプルを発見するため、シグネチャは常に更新が必要です。

技術参考資料と出典

この学習ガイドとインタラクティブなパズルは、世界のNIST、OWASP、およびデータプライバシー・コンプライアンスの標準をもとに作成されています。

学術・業界の参考資料

[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

解答: チェックポイント 1 – 多肢選択

1 問題 1 正解: A

指導メモ

トロイの木馬を特徴づけるものは何ですか? → 正規のソフトウェアを装い、ユーザーをだまして実行させる

2 問題 2 正解: A

指導メモ

ファイルを暗号化して支払いを要求するマルウェアの種類はどれですか? → ランサムウェア

3 問題 3 正解: A

指導メモ

スパイウェアに当たるものは何ですか? → ユーザーのキー入力とブラウザーでの操作をひそかに監視するよう設計されたマルウェア

4 問題 4 正解: A

指導メモ

マルウェアの開発者がルートキットを使うのはなぜですか? → 実行中のプロセスや悪意のあるファイルをOSから隠すため

5 問題 5 正解: A

指導メモ

マルウェア分析で、サンドボックス化とはどういう意味ですか? → 隔離された仮想の保管庫で不審なファイルを実行し、動作を安全に観察する

解答: チェックポイント 2 – 正誤問題

6 問題 6

正解: 誤り

指導メモ

誤り: ワームは自己複製し、ユーザーの操作なしにネットワーク全体に広がります。

7 問題 7

正解: 誤り

指導メモ

誤り: アドウェアは必ずしも無害ではありません。多くは広告を表示するために閲覧状況を追跡します。

8 問題 8

正解: 正しい

指導メモ

正しい: クリーンなオフラインバックアップがあれば身代金を支払わずに暗号化されたファイルを復元できますが、盗まれたデータが漏えいする可能性は残ります。

9 問題 9

正解: 誤り

指導メモ

誤り: シグネチャ型のスキャナーには既知のサンプルが必要なため、まったく新しいゼロデイのマルウェアはすり抜ける可能性があります。

10 問題 10

正解: 正しい

指導メモ

ファイルレスマルウェアは、ディスクにファイルを書き込まず、システムメモリ内で悪意のあるスクリプトを実行します。

用語解答と採点基準

教師用採点基準: 正しい組み合わせ 1 つにつき 1 点(合計 8 点)、文脈の用語 1 つにつき 1 点(合計 6 点)を与えてください。

チェックポイント 4: 解答 – 概念マッチング

D 1. トロイの木馬	F 2. ランサムウェア	A 3. スパイウェア	H 4. ルートキット
G 5. サンドボックス	C 6. 封じ込め	E 7. ワーム	B 8. ファイルレス

チェックポイント 3: 解答 – 重要用語

1 トロイの木馬	2 ランサムウェア	3 スパイウェア	4 ルートキット
5 サンドボックス	6 封じ込め		

チェックポイント 6 代替活動: 解答 – 用語マッチング

1 D – ルートキツト	2 F – フウジコメ	3 H – フアイルレス	4 G – ワーム
5 B – ランサムウエア	6 C – スパイウエア	7 A – トロイノモクバ	8 E – サンドボツクス

指導者向けディスカッションメモ

重要用語:
生徒がトロイの木馬、ランサムウェア、スパイウェアを自分の言葉で説明し、それぞれの例を挙げられるか確認してください。

ケーススタディ:
生徒には、意見ではなくワークシートの事実を根拠に提案するよう促してください。

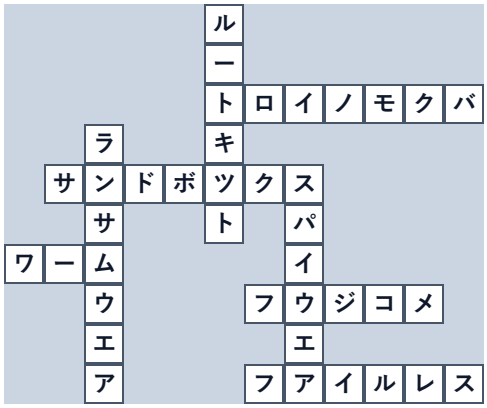
情報源の評価:
ワークシートの参考資料で少なくとも 1 つの主張を確かめさせ、数値・価格・規則が時間とともに変わりうる理由を話し合わせてください。

パズルの解答と指導者用メモ

ワードサーチの解答

ペ	ロ	ボ	タ	レ	ミ	ク	グ	ヌ	チ	ユ	ガ	メ	ロ	ボ
ワ	ラ	メ	キ	ゼ	ゴ	ザ	ス	ス	ホ	フ	ノ	オ	ア	オ
キ	ル	コ	パ	ホ	ヒ	パ	ヘ	ボ	パ	ア	ズ	フ	サ	ン
メ	ハ	ジ	ト	ツ	キ	ト	ー	ル	コ	イ	ヌ	ヤ	モ	ヘ
ワ	レ	ウ	テ	モ	ト	モ	ン	ギ	ゲ	ル	ウ	ズ	ジ	ツ
ス	カ	フ	ゴ	ワ	ロ	ラ	ラ	ニ	グ	レ	カ	エ	バ	コ
ク	ザ	ペ	ダ	キ	イ	ポ	バ	ン	タ	ス	フ	ト	ア	ー
ツ	コ	モ	サ	ガ	ノ	ベ	レ	カ	サ	ゾ	エ	ア	ー	ユ
ボ	コ	ヘ	イ	サ	モ	ラ	サ	ソ	テ	ム	ヌ	コ	ギ	ン
ド	メ	ス	ヌ	グ	ク	ポ	ゴ	ソ	ガ	ド	ウ	セ	イ	イ
ン	ガ	リ	ヤ	レ	バ	ズ	ボ	ワ	ヒ	グ	ゼ	エ	ゲ	ケ
サ	ヤ	プ	オ	タ	グ	ベ	ブ	ノ	ム	イ	ギ	ー	ア	ピ
ピ	マ	ツ	ヌ	メ	ガ	ヒ	ム	ー	ミ	ジ	リ	ト	ロ	ン
テ	ー	ウ	ラ	デ	チ	ダ	ワ	カ	プ	グ	プ	オ	ト	ミ
ー	ツ	ハ	ヨ	レ	ユ	ブ	キ	ム	ー	プ	チ	ピ	リ	ビ

クロスワードの解答



クロスワード解答の教師用ガイド

ヨコのカギ

2 ヨコ: トロイノモクバ 無害または便利なユーティリティプログラムに見せかけた悪意のあるソフトウェア (7 文字)

4 ヨコ: サンドボツクス 悪意のあるファイルを安全に解析するための隔離された仮想環境 (7 文字)

6 ヨコ: ワーム 人の操作なしにネットワーク上で広がる、自己複製型のマルウェア (3 文字)

7 ヨコ: フウジコメ 脅威のペイロードが広がらないよう、感染した端末を制限すること (5 文字)

8 ヨコ: フアイルレス ディスクスキャナーによる検出を避けるため、RAM上で直接実行されるマルウェア (6 文字)

タテのカギ

1 タテ: ルートキット システムのカーネルの奥深くに潜み、管理者権限を維持し続ける隠蔽型マルウェア (6 文字)

3 タテ: ランサムウエア システムのストレージを暗号化し、鍵の引き渡しと引き換えに金銭を要求するマルウェア (7 文字)

5 タテ: スパイウエア ユーザーの操作や入力を密かに監視して記録するよう作られたプログラム (6 文字)

文字並べ替えと暗号解読の解答

単語の並べ替え活動と「秘密の暗号チャレンジ」の採点用の解答。

文字並べ替えの解答

1. ノクトモバイロ — トロイノモクバ
2. アスイエウパ — スパイウエア
3. ボサツスドクン — サンドボツクス
4. ームワ — ワーム
5. ウアムサラエン — ランサムウエア
6. ツキルトトー — ルートキツト
7. コメフジウ — フウジコメ
8. イスフレルア — フアイルレス

秘密の暗号チャレンジ 解答

"タンマツノ フルマイヲ カンシシテ ケンチスル"

ケーススタディの解答

A ケーススタディ 1: 企業でのランサムウェアのペイロードの封じ込め 教師用解答

採点ガイドライン

学生の解答には、次の点を含めてください:

- シナリオ分析: 企業のローカルエリアネットワークが、稼働中のランサムウェアに侵害されました。主要なファイルサーバーで、ファイルの拡張子が .locked と表示され始めています。封じ込めのポリシーを策定してください。
- 推奨される対策と解決策: 影響を受けたすべてのサーバーをローカルエリアネットワークから切断します。アクティブな管理セッションを終了します。安全で書き込みロックされたオフラインバックアップシステムから、侵害されていないファイルを復元します。

B ケーススタディ 2: ファイルレスマルウェアによるメモリインジェクション 教師用解答

採点ガイドライン

学生の解答には、次の点を含めてください:

- シナリオ分析: アナリストが、標準的な管理ツールを使って揮発性のシステム RAM 上で直接実行されている疑わしいスクリプトのパターンを検出しますが、ディスク上には悪意のあるファイルが存在しません。
- 推奨される戦略と解決策: 影響を受けたエンドポイントを隔離し、まずメモリイメージを取得します。PowerShell と WMI のログを確認し、AppLocker で未承認のスクリプトをブロックしてから、再起動してペイロードを消去します。