이름: _____ 날짜: _____ 점수: _____

악성코드 분석 및 위협 완화 가이드

트로이 목마, 랜섬웨어, 스파이웨어, 루트킷, 가상화 샌드박스, 격리

악성코드 분석 학습 개요

보호됨
데이터 암호화
256비트 AES 표준

규정 준수
글로벌 표준
GDPR 및 CCPA 규정 체계

제로 트러스트
접근 정책
다중 요소 인증

환영합니다! 이 활동 자료집은 악성코드 분석과 예방을 안내합니다. 스파이웨어, 트로이 목마, 랜섬웨어 페이로드, 리버스 엔지니어링 도구, 루트킷 동작, 격리 전략을 살펴봅니다.

워크시트 체크포인트

- [ ] **파트 1-4: 사이버 보안과 위협 예방을 익힙니다.**
- [ ] **파트 5-7: 십자말풀이와 단어 찾기 퍼즐을 풉니다.**
- [ ] **파트 8-9: 사례 연구와 암호 도전 과제를 풉니다.**
- [ ] **파트 10: 기초 및 심화 FAQ 페이지를 살펴봅니다.**
- [ ] **파트 11: 흥미로운 실제 사실 10가지를 살펴봅니다.**
- [ ] **보너스: 빠르게 생각하기 도전**

VPN.com 사이버 보안 가이드 열기

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

나의 악성코드 대응 학습 로드맵

- 트로이 목마, 웜, 루트킷 악성코드 유형을 구분하세요.
- 코드 분석을 위한 샌드박스 가상화 실행 환경을 도입하세요.
- 활성 랜섬웨어 페이로드의 격리 및 무해화 계획을 설계하세요.

악성코드 분석 가이드 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. 악성코드 대응에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

악성코드 분석 및 위협 차단(입문)

트로이 목마, 웜, 랜섬웨어 같은 악성 코드는 엔드포인트와 서버에 큰 영향을 미치는 위협입니다. 보안 팀은 가상 샌드박스 안에서 악성코드를 분석하고, 페이로드 확산을 막기 위해 신속한 네트워크 격리 조치를 실행합니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1 1. 트로이 목마의 결정적인 특징은 무엇입니까?

- A. 정상 소프트웨어로 위장해 사용자가 실행하도록 속임
- B. 로컬 네트워크 회선을 따라 자동으로 복제된다
- C. 격리된 가상 샌드박스 안의 파일을 감염시킨다
- D. 인터넷 서비스 제공업체의 트래픽을 가로챈다

2 2. 파일을 암호화하고 대가를 요구하는 악성코드 유형은 무엇입니까?

- A. 랜섬웨어
- B. 스파이웨어
- C. 루트킷
- D. 애드웨어

3 3. 스파이웨어를 나타내는 것은 무엇입니까?

- A. 사용자 키 입력과 브라우저 활동을 몰래 감시하도록 설계된 악성코드
- B. 샌드박스 가상 컨테이너 안에서 실행되는 프로그램 코드
- C. 데이터베이스 레지스트리에서 내려받은 안티 멀웨어 업데이트
- D. 자동 화면 밝기 조절

4 4. 악성코드 개발자가 루트킷을 사용하는 이유는 무엇입니까?

- A. 운영 체제에서 실행 중인 프로세스와 악성 파일을 숨기기 위해
- B. 엔드포인트의 CPU 처리 속도를 높이기 위해
- C. 데이터베이스 파일을 안전한 클라우드 보관소에 백업하려고
- D. 노트북 배터리 수명을 늘리려고

5 5. 악성코드 분석에서 샌드박싱은 무엇을 의미합니까?

- A. 의심스러운 파일을 격리된 가상 보관소에서 실행해 동작을 안전하게 관찰함
- B. 알려진 위협 데이터베이스와 파일 해시 대조하기
- C. 침입 후 데이터베이스 백업 복원하기
- D. 로컬 네트워크 라우터를 공용 회선에서 분리하기

체크포인트 2: 참/거짓 도전

6 질문 6

6. 컴퓨터 웜이 로컬 네트워크로 퍼지려면 사용자의 조작이 필요합니다.

○ 참 ○ 거짓

7 질문 7

7. 애드웨어는 항상 무해하며 사용자 행동이나 브라우저 기록을 추적하지 않습니다.

○ 참 ○ 거짓

8 질문 8

8. 깨끗한 오프라인 백업을 복원하면 피해자는 몸값을 지불하지 않고도 암호화된 파일을 복구할 수 있습니다.

○ 참 ○ 거짓

9 질문 9

9. 시그니처 기반 백신은 제로데이 악성코드의 시그니처가 생기기 전에도 이를 안정적으로 차단합니다.

○ 참 ○ 거짓

10 질문 10

10. 파일리스 악성코드는 디스크에 파일을 쓰지 않고 시스템 메모리에서 악성 스크립트를 실행합니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

아래 각 문장을 읽고 단어 목록에서 알맞은 용어를 골라 빈칸을 채우세요.

1. 안전한 유틸리티 프로그램으로 위장한 악성코드는 _____ 입니다.
2. 금전을 노리고 데이터베이스 시스템을 잠가 버리는 악성 페이로드는 _____ 에 해당합니다.
3. 키로거가 비밀번호를 몰래 기록하는 것은 _____ 에 해당합니다.
4. 운영체제 커널 깊숙이 숨으려면 _____ 이(가) 필요합니다.
5. 의심스러운 파일을 격리된 보관소에서 분석할 때는 가상 _____ 을(를) 사용합니다.
6. 활성 악성코드 페이로드의 확산을 막으려면 즉각적인 네트워크 _____ 이(가) 필요합니다.

어휘 단어 목록

격리 랜섬웨어 루트킷 샌드박스 스파이웨어 트로이 목마 파일리스 WORM

여기에 답을 쓰세요:

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

체크포인트 4: 보안 개념 연결

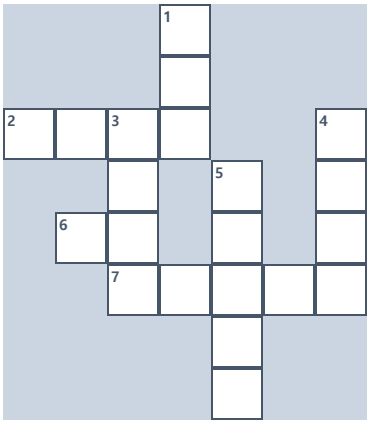
정의 연결하기

왼쪽의 각 어휘를 오른쪽의 알맞은 설명과 연결하고, 입력 칸에 해당하는 글자(A-H)를 쓰세요.

☐	**1. 트로이 목마**	**A**	사용자 활동과 입력을 몰래 감시하고 기록하도록 설계된 프로그램.
☐	**2. 랜섬웨어**	**B**	디스크 검사기의 탐지를 피하기 위해 RAM에서 직접 실행되는 악성코드.
☐	**3. 스파이웨어**	**C**	위협 페이로드가 퍼지지 않도록 감염된 엔드포인트를 제한하는 것.
☐	**4. 루트킷**	**D**	무해하거나 유용한 유틸리티 프로그램으로 위장한 악성 소프트웨어.
☐	**5. 샌드박스**	**E**	사람의 조작 없이 네트워크를 통해 퍼지는 자기 복제 악성코드.
☐	**6. 차단**	**F**	시스템 저장소를 암호화하고 키를 넘겨주는 대가로 대금을 요구하는 악성코드.
☐	**7. 웜**	**G**	악성 파일을 안전하게 분석하는 데 사용하는 격리된 가상 환경.
☐	**8. 파일리스**	**H**	관리자 권한을 유지하기 위해 시스템 커널 깊숙이 숨어 있는 스텔스 악성코드.

체크포인트 5: 십자말풀이

활성화된 흰색 칸에 글자를 입력해 십자말풀이를 푸세요. 숫자는 아래 열쇠에 해당합니다.



가로

2. 이메일에 함께 붙여 보내는 파일 (4)

6. 감염된 기기를 네트워크에서 떼어 내 피해가 번지지 않게 하는 조치 (2)

7. 사용자의 활동과 입력을 몰래 지켜보고 기록하는 악성 프로그램 (5)

세로

1. 인터넷으로 주고받는 전자 우편 (3)

3. 디스크에 파일을 남기지 않고 메모리에서 실행되는 방식의 악성코드 (4)

4. 데이터를 암호로 잠가 놓고 풀어 주는 대가로 돈을 요구하는 악성코드 (4)

5. 유용한 프로그램인 척 위장해 몰래 설치되는 악성 소프트웨어 (5)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

화면 낭독기와 키보드 사용자는 아래 입력란에 십자말풀이 정답을 직접 입력할 수 있습니다.

가로

2 가로: 이메일에 함께 붙여 보내는 파일 (4 글자):

6 가로: 감염된 기기를 네트워크에서 떼어 내 피해가 번지지 않게 하는 조치 (2 글자):

7 가로: 사용자의 활동과 입력을 몰래 지켜보고 기록하는 악성 프로그램 (5 글자):

세로

1 세로: 인터넷으로 주고받는 전자 우편 (3 글자):

3 세로: 디스크에 파일을 남기지 않고 메모리에서 실행되는 방식의 악성코드 (4 글자):

4 세로: 데이터를 암호로 잠가 놓고 풀어 주는 대가로 돈을 요구하는 악성코드 (4 글자):

5 세로: 유용한 프로그램인 척 위장해 몰래 설치되는 악성 소프트웨어 (5 글자):

체크포인트 6: 숨은 단어 찾기

아래 격자에 숨어 있는 핵심 어휘 8개를 찾으세요. 단어는 가로, 세로, 대각선으로 배치될 수 있습니다.

답	메	박	라	인	요	다	서	어	하	크	로	주	샌	도
타	밀	개	접	화	트	격	밀	이	라	소	카	다	스	방
속	스	크	부	타	파	라	전	크	메	기	메	전	안	연
안	박	격	넷	타	바	스	첨	다	트	일	터	응	용	기
첨	드	결	템	색	스	다	험	넷	파	넷	목	데	드	격
섬	샌	버	공	밀	파	자	파	시	술	네	송	리	격	리
번	격	랜	위	결	이	아	요	일	템	메	하	암	인	바
가	마	아	속	섬	웨	암	넷	일	리	벽	랜	소	방	타
일	관	데	터	타	어	술	전	이	화	스	위	공	워	이
파	이	험	리	템	요	주	트	사	도	위	결	호	스	바
부	트	로	이	목	마	웨	카	도	박	답	아	첨	웨	버
첨	화	크	부	랜	카	전	타	관	목	공	사	청	마	가
부	연	카	벽	섬	나	타	결	타	안	크	술	카	리	험
데	하	술	스	웨	첨	도	안	관	검	보	나	다	관	속
전	공	소	섬	어	위	넷	시	요	스	차	전	샌	마	버

어휘 단어 목록

스파이웨어 · 트로이목마 · 격리 · 랜섬웨어 · 이메일 · 파일리스 · 샌드박스 · 첨부파일

체크포인트 6 대체 활동: 접근성을 고려한 어휘 연결

단어 찾기의 8개 어휘를 각각 알맞은 설명과 연결하고, 빈칸에 글자(A-H)를 쓰세요.

어휘 용어

- **A. 스파이웨어**
- **B. 트로이목마**
- **C. 격리**
- **D. 랜섬웨어**
- **E. 이메일**
- **F. 파일리스**
- **G. 샌드박스**
- **H. 첨부파일**

정의 및 연결 항목

1. 데이터를 암호로 잠가 놓고 풀어 주는 대가로 돈을 요구하는 악성코드.
2. 디스크에 파일을 남기지 않고 메모리에서 실행되는 방식의 악성코드.
3. 이메일에 함께 붙여 보내는 파일.
4. 악성 파일을 안전하게 분석하는 데 쓰는 격리된 가상 공간.
5. 유용한 프로그램인 척 위장해 몰래 설치되는 악성 소프트웨어.
6. 감염된 기기를 네트워크에서 떼어 내 피해가 번지지 않게 하는 조치.
7. 사용자의 활동과 입력을 몰래 지켜보고 기록하는 악성 프로그램.
8. 인터넷으로 주고받는 전자 우편.

체크포인트 7: 뒤섞인 단어 도전

아래 글자를 맞게 배열하여 핵심 사이버 보안 개념과 용어를 알아내세요. 정답을 제공된 입력란에 쓰세요.

1. 웨 이 스 어 파 _____
2. 리 격 _____
3. 일 메 이 _____
4. 스 박 샌 드 _____
5. 이 마 트 목 로 _____
6. 웨 어 랜 섬 _____
7. 리 파 스 일 _____
8. 첨 일 파 부 _____

보너스 활동: 빠르게 생각하기

각 범주마다 답을 3개씩 쓰세요. 목록을 가장 먼저 채운 사람이 이깁니다.

1	안전한 앱을 다운로드할 수 있는 곳			
2	해킹당할 수 있는 기기			
3	백업하는 것			
4	이메일의 경고 신호			
5	휴대폰에 악성코드가 있다는 신호			
6	알고 있는 악성코드의 종류			
7	주의해야 하는 파일 형식			
8	악성코드가 PC에 들어오는 경로			
9	오늘부터 시작할 수 있는 안전 습관			
10	사이버 보안과 관련된 단어			
11	데이터가 유출된 후에 할 일			
12	소프트웨어를 업데이트하는 이유			
13	악성코드와 비슷한 이름을 가진 동물이나 캐릭터			
14	악성코드가 훔칠 수 있는 것			
15	잘못된 링크를 클릭했을 때 할 일			

체크포인트 8: 사이버 보안 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 기업 랜섬웨어 페이로드 차단

👷

상황: 한 기업의 근거리 통신망(LAN)이 활성 랜섬웨어에 침해되었습니다. 주요 파일 서버에서 파일 확장자가 .locked로 표시되기 시작했습니다. 차단 정책을 수립하세요.

토론 질문: 차단 단계를 자세히 설명하고, 데이터 복구 절차를 간략히 설명하세요.

사례 연구 2: 파일리스 악성코드 메모리 인젝션

👷

상황: 한 분석가가 표준 관리 도구를 사용해 휘발성 시스템 RAM에서 직접 실행되는 의심스러운 스크립트 패턴을 발견하지만, 디스크에는 악성 파일이 없습니다.

토론 질문: 메모리 분석 전략을 설명하고, 파일리스 실행을 차단하는 도구를 명시하세요.

체크포인트 9: 암호 해독하기

사이버 보안 전문가는 온라인 위협 행위자로부터 네트워크 자산을 보호합니다. 아래의 자모-숫자 키를 사용해 해당하는 자모를 빈칸에 써서 메시지를 해독하세요.

자모-숫자 암호화 키

ㄱ=1 ㄲ=2 ㄴ=3 ㄷ=4 ㄸ=5 ㄹ=6 ㅁ=7 ㅂ=8 ㅃ=9 ㅅ=10
ㅆ=11 ㅇ=12 ㅈ=13 ㅉ=14 ㅊ=15 ㅋ=16 ㅌ=17 ㅍ=18 ㅎ=19 ㅏ=20
ㅐ=21 ㅑ=22 ㅒ=23 ㅓ=24 ㅔ=25 ㅕ=26 ㅖ=27 ㅗ=28 ㅘ=29 ㅙ=30
ㅚ=31 ㅛ=32 ㅜ=33 ㅝ=34 ㅞ=35 ㅟ=36 ㅠ=37 ㅡ=38 ㅢ=39 ㅣ=40

19	21	12	4	28	12		1	20	7	10	40	6	28		1	20	7	12	26	7

17	20	7	13	40

해독된 메시지:

팁: 각 숫자는 아래 키의 한글 자모 하나를 나타냅니다. 자모를 차례로 모아 글자를 만드세요(예: ㅂ+ㅗ = 보).

체크포인트 10: 기초 사이버 보안 FAQ (파트 A)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q1: 악성코드란 무엇인가요?

공격자가 기기와 네트워크의 데이터를 손상하거나 가로채거나 훔치려고 만든 악성 소프트웨어.

Q2: 바이러스와 웜의 차이는 무엇인가요?

바이러스는 퍼지려면 파일 열기 같은 사람의 행동이 필요하지만, 웜은 네트워크를 통해 자동으로 퍼집니다.

Q3: 트로이 목마는 컴퓨터를 어떻게 감염시키나요?

무해하거나 안전한 프로그램인 것처럼 가장하여 악성 페이로드를 숨기는 방식으로 사용자를 속입니다.

Q4: 랜섬웨어란 무엇인가요?

대상 시스템의 파일을 암호화하고 복호화 키를 대가로 금전을 요구하는 악성코드의 한 종류. [1]

Q5: 스파이웨어란 무엇인가요?

사용자의 키 입력, 비밀번호, 탐색 습관을 몰래 기록해 공격자에게 보내는 악성 소프트웨어.

체크포인트 10: 기초 사이버 보안 FAQ (파트 B)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q6: 샌드박싱이란 무슨 뜻인가요?

운영 시스템에 위험을 주지 않고 동작을 관찰하기 위해 의심스러운 파일을 안전하게 격리된 가상 환경에서 실행하는 것.

Q7: 파일리스 악성코드란 무엇인가요?

정상적인 유틸리티를 이용해 시스템 메모리(RAM)에서 직접 실행되며, 기본적인 검사기를 피하려고 디스크에 파일을 쓰지 않는 악성코드.

Q8: 루트킷은 악성코드를 어떻게 보호하나요?

악성 프로세스와 파일을 숨기며, 흔히 운영체제 커널을 변조하므로 바이러스 백신 스캐너가 놓칠 수 있습니다.

Q9: 동적 동작 모니터링이란 무엇인가요?

실행 중인 프로세스를 실시간으로 감시하여 대량 파일 암호화처럼 악성코드에 전형적인 동작을 차단하는 백신 검사 방식입니다.

Q10: 사고 대응에서 봉쇄가 왜 시급한가요?

침해된 엔드포인트를 격리하면 활성 악성코드 페이로드가 다른 네트워크 기기로 퍼지는 것을 막을 수 있습니다.

체크포인트 10: 심화 보안 FAQ (파트 C)

보안 프레임워크, 악성코드 분석, 데이터 규정 준수의 고급 기술적 측면을 탐구합니다.

Q1: 악성코드 개발자는 시그니처 기반 백신 스캐너를 어떻게 우회하나요?

다형성을 사용하여 감염될 때마다 파일의 해시와 코드 구조를 바꾸면서도 악성 동작은 그대로 유지합니다.

Q2: 악성코드 캠페인에서 이중 용도 도구의 위험은 무엇인가요?

공격자는 PowerShell이나 Sysinternals 같은 정상적인 관리 도구를 사용해 평범한 네트워크 트래픽에 섞여 들어가므로 탐지가 어렵습니다.

Q3: 프로세스 할로잉은 악성 페이로드를 어떻게 실행하나요?

정상적인 시스템 프로세스를 일시 중단 상태로 실행하고, 메모리 코드를 악성코드로 바꾼 뒤 실행을 재개합니다.

Q4: 명령 및 제어(C2) 서버의 역할은 무엇인가요?

해커가 운영하며 감염된 기기에서 실행 중인 악성코드에 명령과 페이로드를 보내는 원격 서버.

Q5: 키로깅을 탐지하기 어려운 이유는 무엇인가요?

기본적인 키로거는 CPU 자원을 거의 쓰지 않고 정상적인 사용자 공간 유틸리티 안에 프로세스를 숨깁니다.

체크포인트 10: 심화 보안 FAQ (파트 D)

보안 프레임워크, 악성코드 분석, 데이터 규정 준수의 고급 기술적 측면을 탐구합니다.

Q6: 코드 난독화는 악성코드 분석을 어떻게 지연시키나요?

소스 코드를 암호화하거나 재배열하여 분석 도구와 보안 스캐너가 읽을 수 없게 합니다.

Q7: 부트킷의 기능은 무엇인가요?

부팅 과정(MBR, 부트 섹터, UEFI 펌웨어)을 감염시켜 운영 체제가 로드되기 전에 실행되는 루트킷.

Q8: 휴리스틱 검사는 제로데이 위협을 어떻게 식별하나요?

일치하는 데이터베이스 해시를 찾는 대신 의심스러운 코드 패턴과 관리자 명령을 검사합니다.

Q9: DLL 하이재킹의 위협은 무엇인가요?

악성 동적 연결 라이브러리(DLL)를 정상 애플리케이션의 디렉터리 경로에 넣어 그 애플리케이션이 불러오게 만드는 것.

Q10: 자동화된 악성코드 분석 파이프라인은 가상화를 어떻게 활용하나요?

의심스러운 파일을 여러 OS 가상 머신에서 실행하여 동작 로그와 네트워크 PCAP 파일을 자동으로 생성합니다.

파트 11: 실제 사이버 보안 사실 10가지와 시사점

보안 침해, 방어 메커니즘, 규정 준수 표준에 관한 실제 사실을 살펴보세요.

1. 보안 인사이트

트로이 목마는 악성 코드를 무해해 보이는 프로그램 안에 숨기기 때문에 여전히 흔한 감염 방법입니다.

2. 보안 인사이트

FBI의 IC3는 2025년에 3,600건이 넘는 랜섬웨어 신고를 접수했으며, 보고된 피해액은 $32 million를 넘었습니다. [3]

3. 보안 인사이트

웜은 SMB의 EternalBlue처럼 패치되지 않은 프로토콜 취약점을 악용해 네트워크 전반으로 빠르게 퍼질 수 있습니다.

4. 보안 인사이트

파일리스 악성코드는 정상적인 도구를 통해 메모리에서 실행되고 디스크에 흔적을 거의 남기지 않으므로 탐지하기 어렵습니다.

5. 보안 인사이트

분석 샌드박스는 보통 실행할 때마다 깨끗한 스냅샷으로 되돌아가므로 모든 테스트가 알려진 상태에서 시작됩니다.

6. 보안 인사이트

루트킷은 커널 시스템 호출을 수정해 악성코드 검사기에 거짓 진단 결과를 보고할 수 있습니다.

7. 보안 인사이트

코드 난독화는 패커 유틸리티를 사용해 악성코드의 실제 바이너리 페이로드 구조를 압축하고 숨깁니다.

8. 보안 인사이트

다형성 악성코드는 새 복사본마다 코드를, 따라서 파일 해시를 바꿔 시그니처 검사를 회피합니다.

9. 보안 인사이트

DLL 하이재킹은 Windows와 같은 일반 운영체제의 검색 순서 설정을 악용합니다.

10. 보안 인사이트

보안 업체들은 매일 엄청난 수의 새 악성코드 샘플을 발견하므로 시그니처를 계속 업데이트해야 합니다.

기술 참고 자료 및 출처

이 학습 가이드와 인터랙티브 퍼즐은 전 세계 NIST, OWASP, 개인정보 보호 규정 준수 표준을 바탕으로 만들었습니다.

학술 및 업계 참고 자료

[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

답안: 체크포인트 1 – 객관식

1 질문 1 정답: A

교사용 참고

트로이 목마의 결정적인 특징은 무엇입니까? → 정상 소프트웨어로 위장해 사용자가 실행하도록 속임

2 질문 2 정답: A

교사용 참고

파일을 암호화하고 대가를 요구하는 악성코드 유형은 무엇입니까? → 랜섬웨어

3 질문 3 정답: A

교사용 참고

스파이웨어를 나타내는 것은 무엇입니까? → 사용자 키 입력과 브라우저 활동을 몰래 감시하도록 설계된 악성코드

4 질문 4 정답: A

교사용 참고

악성코드 개발자가 루트킷을 사용하는 이유는 무엇입니까? → 운영 체제에서 실행 중인 프로세스와 악성 파일을 숨기기 위해

5 질문 5 정답: A

교사용 참고

악성코드 분석에서 샌드박싱은 무엇을 의미합니까? → 의심스러운 파일을 격리된 가상 보관소에서 실행해 동작을 안전하게 관찰함

답안: 체크포인트 2 – 참 또는 거짓

6 **질문 6** 정답: 거짓

교사용 참고

거짓: 웜은 스스로 복제하며 사용자의 어떤 조작 없이도 네트워크를 통해 퍼집니다.

7 **질문 7** 정답: 거짓

교사용 참고

거짓: 애드웨어가 항상 무해한 것은 아니며, 상당수는 광고 타기팅을 위해 인터넷 사용 기록을 추적합니다.

8 **질문 8** 정답: 참

교사용 참고

참: 깨끗한 오프라인 백업은 몸값 없이도 암호화된 파일을 복원하지만, 도난당한 데이터는 여전히 유출될 수 있습니다.

9 **질문 9** 정답: 거짓

교사용 참고

거짓: 시그니처 스캐너는 알려진 샘플이 필요하므로, 완전히 새로운 제로데이 악성코드는 이를 피해 갈 수 있습니다.

10 **질문 10** 정답: 참

교사용 참고

파일리스 악성코드는 디스크에 파일을 쓰지 않고 시스템 메모리에서 악성 스크립트를 실행합니다.

어휘 정답 및 채점 기준표

교사용 채점 기준: 정확하게 연결한 항목마다 1점(총 8점), 문맥 용어마다 1점(총 6점)을 줍니다.

체크포인트 4: 답안 – 개념 연결

D 1. 트로이 목마	F 2. 랜섬웨어	A 3. 스파이웨어	H 4. 루트킷
G 5. 샌드박스	C 6. 차단	E 7. 웜	B 8. 파일리스

체크포인트 3: 답안 – 핵심 용어

1 트로이 목마	2 랜섬웨어	3 스파이웨어	4 루트킷
5 샌드박스	6 격리		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 D – 랜섬웨어	2 F – 파일리스	3 H – 첨부파일	4 G – 샌드박스
5 B – 트로이목마	6 C – 격리	7 A – 스파이웨어	8 E – 이메일

교사를 위한 토론 참고

핵심 용어:
학생들이 트로이 목마, 랜섬웨어, 스파이웨어를 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

사례 연구:
학생들이 의견이 아니라 워크시트의 사실을 근거로 권고안을 제시하게 하세요.

출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

답	메	박	라	인	요	다	서	어	하	크	로	주	샌	도
타	밀	개	접	화	트	격	밀	이	라	소	카	다	스	방
속	스	크	부	타	파	라	전	크	메	기	메	전	안	연
안	박	격	넷	타	바	스	첨	다	트	일	터	응	용	기
첨	드	결	템	색	스	다	험	넷	파	넷	목	데	드	격
섬	샌	버	공	밀	파	자	파	시	술	네	송	리	격	리
번	격	랜	위	결	이	아	요	일	템	메	하	암	인	바
가	마	아	속	섬	웨	암	넷	일	리	벽	랜	소	방	타
일	관	데	터	타	어	술	전	이	화	스	위	공	워	이
파	이	험	리	템	요	주	트	사	도	위	결	호	스	바
부	트	로	이	목	마	웨	카	도	박	답	아	첨	웨	버
첨	화	크	부	랜	카	전	타	관	목	공	사	청	마	가
부	연	카	벽	섬	나	타	결	타	안	크	술	카	리	험
데	하	술	스	웨	첨	도	안	관	검	보	나	다	관	속
전	공	소	섬	어	위	넷	시	요	스	차	전	샌	마	버

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

2 가로: 첨부파일 이메일에 함께 붙여 보내는 파일 (4 글자)

6 가로: 격리 감염된 기기를 네트워크에서 떼어 내 피해가 번지지 않게 하는 조치 (2 글자)

7 가로: 스파이웨어 사용자의 활동과 입력을 몰래 지켜보고 기록하는 악성 프로그램 (5 글자)

세로

1 세로: 이메일 인터넷으로 주고받는 전자 우편 (3 글자)

3 세로: 파일리스 디스크에 파일을 남기지 않고 메모리에서 실행되는 방식의 악성코드 (4 글자)

4 세로: 랜섬웨어 데이터를 암호로 잠가 놓고 풀어 주는 대가로 돈을 요구하는 악성코드 (4 글자)

5 세로: 트로이목마 유용한 프로그램인 척 위장해 몰래 설치되는 악성 소프트웨어 (5 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 웨이스어파 — **스파이웨어**
2. 리격 — **격리**
3. 일메이 — **이메일**
4. 스박샌드 — **샌드박스**
5. 이마트목로 — **트로이목마**
6. 웨어랜섬 — **랜섬웨어**
7. 리파스일 — **파일리스**
8. 첨일파부 — **첨부파일**

비밀 암호 도전 정답

"행동 감시로 감염 탐지"

사례 연구 답안

A 사례 연구 1: 기업 랜섬웨어 페이로드 차단

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 기업 로컬 영역 네트워크가 활성 랜섬웨어에 침해되었습니다. 주요 파일 서버에서 파일 확장자가 .locked로 표시되기 시작했습니다. 격리 정책을 수립하세요.
- 권장 전략 및 해결책: 영향을 받은 모든 서버를 로컬 영역 네트워크에서 분리합니다. 활성 관리자 세션을 종료합니다. 쓰기가 잠긴 안전한 오프라인 백업 시스템에서 손상되지 않은 파일을 복원합니다.

B 사례 연구 2: 파일리스 악성코드 메모리 인젝션

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 한 분석가가 표준 관리 도구를 사용해 휘발성 시스템 RAM에서 직접 실행되는 의심스러운 스크립트 패턴을 탐지했지만, 디스크에는 악성 파일이 없습니다.
- 권장 전략 및 해결책: 영향을 받은 엔드포인트를 격리하고 먼저 메모리 이미지를 확보하세요. PowerShell과 WMI 로그를 검토하고 AppLocker로 승인되지 않은 스크립트를 차단한 뒤, 재부팅해 페이로드를 제거합니다.