Imię i nazwisko: _____ **Data:** _____ **Wynik:** _____

Analiza złośliwego oprogramowania i ograniczanie zagrożeń Przewodnik

Trojany, ransomware, oprogramowanie szpiegujące, rootkity, piaskownice wirtualizacji, izolacja

PRZEGLĄD NAUKOWY: ANALIZA ZŁOŚLIWEGO OPROGRAMOWANIA

CHRONIONY
SZYFROWANIE DANYCH
Standard AES 256-bitowy

ZGODNY
STANDARDY GLOBALNE
Ramy prawne RODO (GDPR) i CCPA

ZERO TRUST
POLITYKA DOSTĘPU
Uwierzytelnianie wieloskładnikowe

Witaj! Ten pakiet ćwiczeń przeprowadzi cię przez analizę złośliwego oprogramowania i zapobieganie mu. Poznasz oprogramowanie szpiegujące, trojany, ładunki ransomware, narzędzia inżynierii wstecznej, zachowanie rootkitów i strategie izolowania zagrożeń.

PUNKTY KONTROLNE KARTY PRACY

- [ ] **Część 1–4: Opanuj cyberbezpieczeństwo i zapobieganie zagrożeniom.**
- [ ] **Część 5–7: Rozwiąż krzyżówkę i wykreślankę.**
- [ ] **Część 8–9: Rozwiąż studia przypadków i wyzwanie z szyfrem.**
- [ ] **Część 10: Przejrzyj strony z podstawowymi i zaawansowanymi najczęściej zadawanymi pytaniami.**
- [ ] **Część 11: Poznaj 10 ciekawych faktów z praktyki.**
- [ ] **Bonus: wyzwanie Myśl szybko.**

Otwórz przewodnik VPN.com po cyberbezpieczeństwie

URL: https://www.vpn.com/pl/cyberbezpieczenstwo/malware/

Twoja ścieżka nauki: ograniczanie skutków złośliwego oprogramowania

- Rozróżnij typy złośliwego oprogramowania: trojan, robak i rootkit.
- Wdróż uruchamianie kodu w wirtualizowanej piaskownicy (sandbox) na potrzeby jego analizy.
- Zaprojektuj plany izolowania i oczyszczania aktywnych ładunków ransomware.

INSTRUKCJE: PRZEWODNIK PO ANALIZIE ZŁOŚLIWEGO OPROGRAMOWANIA

Odpowiedz na pytania testu wielokrotnego wyboru oraz pytania prawda/fałsz, uzupełnij zdania z lukami za pomocą banku wyrazów, dopasuj definicje i rozwiąż krzyżówkę oraz wykreślankę. Zastosuj swoją wiedzę z zakresu ograniczania skutków złośliwego oprogramowania. Zakończ zadaniem dodatkowym Myśl szybko.

ANALIZA ZŁOŚLIWEGO OPROGRAMOWANIA I OGRANICZANIE ZAGROŻEŃ (WPROWADZENIE)

Złośliwy kod, taki jak trojany, robaki i ransomware, stanowi poważne zagrożenie dla punktów końcowych i serwerów. Zespoły ds. bezpieczeństwa analizują złośliwe oprogramowanie w wirtualnych piaskownicach i szybko izolują sieć, aby powstrzymać rozprzestrzenianie się ładunku.

PRZECZYTAJ UWAŻNIE KAŻDY PUNKT KONTROLNY I WYBIERZ LUB NAPISZ POPRAWNĄ ODPOWIEDŹ.

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. **1. Jaka jest cecha charakterystyczna konia trojańskiego?**
   - A. Podszywa się pod legalne oprogramowanie, aby nakłonić użytkowników do jego uruchomienia
   - B. Replikuje się automatycznie przez łącza sieci lokalnej
   - C. Infekuje pliki w izolowanych wirtualnych piaskownicach
   - D. Przechwytuje ruch dostawcy internetu

2. **2. Który typ złośliwego oprogramowania szyfruje pliki i żąda zapłaty?**
   - A. Ransomware
   - B. Oprogramowanie szpiegujące
   - C. Rootkit
   - D. Adware

3. **3. Co reprezentuje oprogramowanie szpiegujące (spyware)?**
   - A. Złośliwe oprogramowanie zaprojektowane do potajemnego monitorowania naciśnięć klawiszy i aktywności w przeglądarce
   - B. Kod programu wykonywany wewnątrz kontenera wirtualnego w piaskownicy
   - C. Aktualizacje antymalware pobierane z rejestrów baz danych
   - D. Automatyczne dostosowanie jasności ekranu

4. **4. Dlaczego twórcy złośliwego oprogramowania używają rootkitów?**
   - A. Aby ukryć aktywne procesy i złośliwe pliki przed systemem operacyjnym
   - B. Aby zwiększyć szybkość przetwarzania procesora na punktach końcowych
   - C. Aby tworzyć kopie zapasowe plików bazy danych w bezpiecznych skarbcach w chmurze
   - D. Aby poprawić czas pracy baterii w laptopach

5. **5. Co oznacza sandboxing w analizie złośliwego oprogramowania?**
   - A. Uruchamianie podejrzanych plików w izolowanym wirtualnym skarbcu, aby bezpiecznie obserwować ich zachowanie
   - B. Skanowanie skrótów plików pod kątem znanych baz zagrożeń
   - C. Przywracanie kopii zapasowych bazy danych po włamaniu
   - D. Odłączanie lokalnych routerów sieciowych od linii publicznych

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. Robaki komputerowe wymagają interakcji użytkownika, aby rozprzestrzeniać się w sieciach lokalnych.

- ○ Prawda
- ○ Fałsz

7 Pytanie 7

7. Adware jest zawsze nieszkodliwe i nie śledzi zachowania użytkownika ani historii przeglądarki.

- ○ Prawda
- ○ Fałsz

8 Pytanie 8

8. Przywrócenie czystych kopii zapasowych offline pozwala ofiarom odzyskać zaszyfrowane pliki bez płacenia okupu.

- ○ Prawda
- ○ Fałsz

9 Pytanie 9

9. Antywirus oparty na sygnaturach niezawodnie zatrzymuje złośliwe oprogramowanie zero-day, zanim powstanie jego sygnatura.

- ○ Prawda
- ○ Fałsz

10 Pytanie 10

10. Złośliwe oprogramowanie bezplikowe wykonuje złośliwe skrypty w pamięci systemu, unikając zapisu plików na dysku.

- ○ Prawda
- ○ Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

Przeczytaj każde poniższe zdanie i uzupełnij lukę poprawnym terminem z banku słów.

1. Złośliwe oprogramowanie podszywające się pod bezpieczny program narzędziowy to _____ .

2. Złośliwe ładunki blokujące systemy baz danych dla okupu to _____ .

3. Keyloggery potajemnie rejestrujące hasła są rodzajem oprogramowania typu _____ .

4. Ukrywanie się głęboko w jądrach systemów operacyjnych jest cechą programu typu _____ .

5. Analizę podejrzanych plików w odizolowanym środowisku umożliwia wirtualna _____ .

6. Aby zatrzymać rozprzestrzenianie się aktywnych ładunków złośliwego oprogramowania, trzeba niezwłocznie przeprowadzić _____ sieci.

BANK SŁÓW

BEZPLIKOWE | IZOLOWANIE | OPROGRAMOWANIE SZPIEGUJĄCE | PIASKOWNICA | RANSOMWARE | ROBAK | ROOTKIT | TROJAN

Wpisz tutaj swoje odpowiedzi:

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

Punkt kontrolny 4: Dopasowywanie pojęć z zakresu bezpieczeństwa

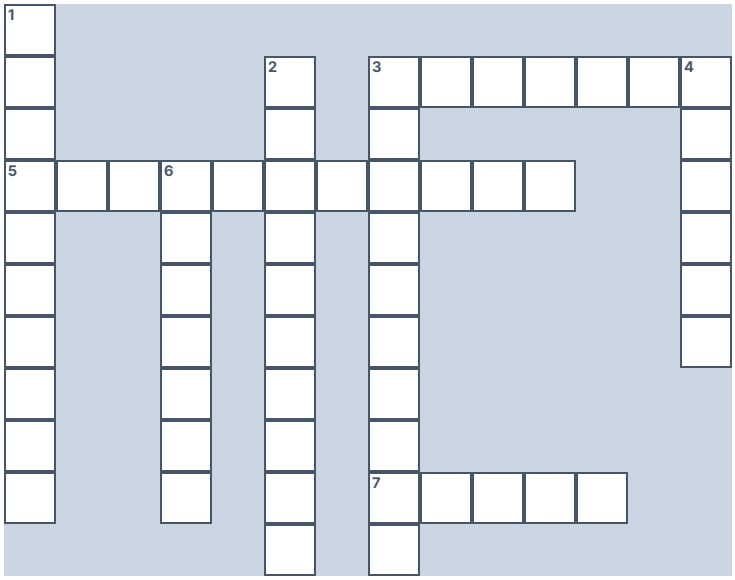
DOPASOWYWANIE DEFINICJI

Dopasuj każde pojęcie po lewej stronie do jego poprawnej definicji po prawej, wpisując odpowiednią literę (A-H) w edytowalne pole.

☐	1. TROJAN	A	Program zaprojektowany do potajemnego monitorowania i rejestrowania aktywności i danych wprowadzanych przez użytkownika.
☐	2. RANSOMWARE	B	Złośliwe oprogramowanie działające bezpośrednio w pamięci RAM, aby uniknąć wykrycia przez skanery dysku.
☐	3. OPROGRAMOWANIE SZPIEGUJĄCE	C	Ograniczanie zainfekowanych punktów końcowych, aby zapobiec rozprzestrzenianiu się ładunków zagrożeń.
☐	4. ROOTKIT	D	Złośliwe oprogramowanie udające nieszkodliwy lub użyteczny program narzędziowy.
☐	5. PIASKOWNICA	E	Samoreplikujące się złośliwe oprogramowanie rozprzestrzeniające się w sieciach bez działania człowieka.
☐	6. OGRANICZENIE	F	Złośliwe oprogramowanie szyfrujące pamięć masową systemu i żądające zapłaty za dostarczenie klucza.
☐	7. ROBAK KOMPUTEROWY	G	Odizolowane środowisko wirtualne służące do bezpiecznej analizy złośliwych plików.
☐	8. BEZPLIKOWE	H	Ukryte złośliwe oprogramowanie głęboko w jądrze systemu, które utrzymuje kontrolę administracyjną.

Punkt kontrolny 5: Krzyżówka

Rozwiąż krzyżówkę, wpisując litery w aktywne białe pola. Numery odpowiadają wskazówkom poniżej.



POZIOMO

3. Ukryte złośliwe oprogramowanie głęboko w jądrach systemów, utrzymujące kontrolę administracyjną. (7)

5. Odizolowane środowisko wirtualne służące do bezpiecznej analizy złośliwych plików. (11)

7. Samoreplikujące się złośliwe oprogramowanie rozprzestrzeniające się w sieciach bez udziału człowieka. (5)

PIONOWO

1. Złośliwe oprogramowanie wykonywane bezpośrednio w pamięci RAM, aby uniknąć wykrycia przez skanery dysków. (10)

2. Ograniczanie zainfekowanych punktów końcowych, aby zapobiec rozprzestrzenianiu się ładunków zagrożeń. (10)

3. Złośliwe oprogramowanie szyfrujące pamięć masową systemu i żądające zapłaty za dostarczenie klucza. (10)

4. Złośliwe oprogramowanie podszywające się pod nieszkodliwy lub użyteczny program narzędziowy. (6)

6. Program zaprojektowany do potajemnego monitorowania i rejestrowania aktywności oraz wprowadzanych danych użytkownika. (7)

Punkt kontrolny 5, wariant alternatywny: Dostępne wskazówki do krzyżówki

Użytkownicy czytników ekranu i klawiatury mogą wpisywać odpowiedzi do krzyżówki bezpośrednio w polach tekstowych poniżej.

POZIOMO

3 poziomo: Ukryte złośliwe oprogramowanie głęboko w jądrach systemów, utrzymujące kontrolę administracyjną. (7 liter):

5 poziomo: Odizolowane środowisko wirtualne służące do bezpiecznej analizy złośliwych plików. (11 liter):

7 poziomo: Samoreplikujące się złośliwe oprogramowanie rozprzestrzeniające się w sieciach bez udziału człowieka. (5 liter):

PIONOWO

1 pionowo: Złośliwe oprogramowanie wykonywane bezpośrednio w pamięci RAM, aby uniknąć wykrycia przez skanery dysków. (10 liter):

2 pionowo: Ograniczanie zainfekowanych punktów końcowych, aby zapobiec rozprzestrzenianiu się ładunków zagrożeń. (10 liter):

3 pionowo: Złośliwe oprogramowanie szyfrujące pamięć masową systemu i żądające zapłaty za dostarczenie klucza. (10 liter):

4 pionowo: Złośliwe oprogramowanie podszywające się pod nieszkodliwy lub użyteczny program narzędziowy. (6 liter):

6 pionowo: Program zaprojektowany do potajemnego monitorowania i rejestrowania aktywności oraz wprowadzanych danych użytkownika. (7 liter):

Punkt kontrolny 6: Ukryte słowa w wykreślance

Znajdź w poniższej siatce 8 kluczowych terminów słownictwa. Wyrazy mogą biec poziomo, pionowo lub po przekątnej.

C R I F Ń R M B P Y P O C U S
Ś E Ł J B A B E C Ó R Z Ł K Z
E L Y T L D Q Z N K O D I Ń N
R L E R A W Y P S Q O Ó G N N
A Q R S T P T L F B T Ś P I O
W H S B W I Ć I Ś Ź K V C Z Ż
M W Ę L G A Ż K Ć N I D Q O Y
O Ó C U B S A O Ż Ń T Ć L L A
S D O D Ę K G W I Ć R Q N O M
N E I S Ż O R E Ś Ę Q A V W E
A A A Q Ó W O N P T J Y Q A K
R R T S Ć N B N Ź O B Ę S N Y
X J A R Ż I A Z R Z Ł F I I N
R K M M T C K T O G P Q G E Ż
Ą O V F V A B Ź S Ź B G M Ż G

LISTA SŁÓW

TROJAN, RANSOMWARE, SPYWARE, ROOTKIT, PIASKOWNICA, IZOLOWANIE, ROBAK, BEZPLIKOWE

Punkt kontrolny 6, wariant alternatywny: Dostępne dopasowywanie słownictwa

Dopasuj każde z 8 pojęć z wykreślanki do jego poprawnej definicji, wpisując literę (A-H) w puste pole.

TERMINY ZE SŁOWNICZKA

- **A. TROJAN**
- **B. RANSOMWARE**
- **C. SPYWARE**
- **D. ROOTKIT**
- **E. PIASKOWNICA**
- **F. IZOLOWANIE**
- **G. ROBAK**
- **H. BEZPLIKOWE**

DEFINICJE I POLA DOPASOWANIA

1. Ukryte złośliwe oprogramowanie głęboko w jądrach systemów, utrzymujące kontrolę administracyjną.
2. Ograniczanie zainfekowanych punktów końcowych, aby zapobiec rozprzestrzenianiu się ładunków zagrożeń.
3. Złośliwe oprogramowanie wykonywane bezpośrednio w pamięci RAM, aby uniknąć wykrycia przez skanery dysków.
4. Samoreplikujące się złośliwe oprogramowanie rozprzestrzeniające się w sieciach bez udziału człowieka.
5. Złośliwe oprogramowanie szyfrujące pamięć masową systemu i żądające zapłaty za dostarczenie klucza.
6. Program zaprojektowany do potajemnego monitorowania i rejestrowania aktywności oraz wprowadzanych danych użytkownika.
7. Złośliwe oprogramowanie podszywające się pod nieszkodliwy lub użyteczny program narzędziowy.
8. Odizolowane środowisko wirtualne służące do bezpiecznej analizy złośliwych plików.

Punkt kontrolny 7: Wyzwanie – pomieszane słowa

Rozszyfruj poniższe litery, aby odkryć kluczowe pojęcia i terminy związane z cyberbezpieczeństwem. Wpisz odpowiedzi w przygotowanych polach.

1. OTJANR
2. SYERAWP
3. PWONAICAKIS
4. BKARO
5. AMEASWORRN
6. IOKRTTO
7. ZLIAWNIEOO
8. WPIEBLEKOZ

Zadanie dodatkowe: Myśl szybko

3 ODPOWIEDZI W KAŻDEJ KATEGORII. WYGRYWA OSOBA, KTÓRA PIERWSZA WYPEŁNI LISTĘ.

1	Miejsca, z których można pobierać bezpieczne aplikacje			
2	Urządzenia, które można zhakować			
3	Rzeczy, z których robisz kopie zapasowe			
4	Sygnały ostrzegawcze w e-mailu			
5	Oznaki, że telefon ma złośliwe oprogramowanie			
6	Rodzaje złośliwego oprogramowania, które znasz			
7	Typy plików, na które trzeba uważać			
8	Sposoby, w jakie złośliwe oprogramowanie trafia na komputer			
9	Bezpieczne nawyki, które możesz zacząć już dziś			
10	Słowa związane z cyberbezpieczeństwem			
11	Rzeczy do zrobienia po wycieku danych			
12	Powody, dla których warto aktualizować oprogramowanie			
13	Zwierzęta lub postacie o nazwach podobnych do złośliwego oprogramowania			
14	Rzeczy, które złośliwe oprogramowanie może ukraść			
15	Rzeczy do zrobienia, jeśli kliknąłeś w zły link			

Punkt kontrolny 8: Studia przypadków z cyberbezpieczeństwa

Zastosuj poznane pojęcia, aby rozwiązać poniższe scenariusze z życia wzięte.

STUDIUM PRZYPADKU 1: OGRANICZANIE ŁADUNKU RANSOMWARE W FIRMIE

👷

Scenariusz: Firmowa sieć lokalna została zaatakowana przez aktywny ransomware. Na kluczowych serwerach plików zaczęły pojawiać się pliki z rozszerzeniem .locked. Ustal zasady powstrzymywania incydentu.

Pytanie do dyskusji: Opisz szczegółowo kroki powstrzymania i przedstaw protokół odzyskiwania danych.

STUDIUM PRZYPADKU 2: BEZPLIKOWE ZŁOŚLIWE OPROGRAMOWANIE WSTRZYKIWANE DO PAMIĘCI

👷

Scenariusz: Analityk wykrywa podejrzane wzorce skryptów wykonujących się bezpośrednio w ulotnej pamięci RAM systemu za pomocą standardowych narzędzi administracyjnych, ale na dysku nie ma żadnych złośliwych plików.

Pytanie do dyskusji: Wyjaśnij strategię analizy pamięci i wskaż narzędzia blokujące wykonywanie bezplikowe.

Punkt kontrolny 9: Odszyfruj szyfr

Specjalista ds. cyberbezpieczeństwa chroni zasoby sieciowe przed cyberprzestępcami. Użyj poniższego klucza liter i liczb, aby odszyfrować wiadomość, wpisując pasujące litery w puste miejsca.

KLUCZ SZYFROWANIA LITERA-LICZBA

A=1 Ą=2 B=3 C=4 Ć=5 D=6 E=7 Ę=8 F=9 G=10 H=11 I=12
J=13 K=14 L=15 Ł=16 M=17 N=18 Ń=19 O=20 Ó=21 P=22 Q=23 R=24
S=25 Ś=26 T=27 U=28 V=29 W=30 X=31 Y=32 Z=33 Ź=34 Ż=35

30	32	14	24	32	30	1	13		16	1	6	28	18	14	12
7	18	6	22	20	12	18	27		17	20	18	12	27	20	24	7	17
33	1	4	11	20	30	1	19										

Odszyfrowana wiadomość:

WSKAZÓWKA: KAŻDA LICZBA OZNACZA POZYCJĘ TEJ LITERY W ALFABECIE (NP. 1 = A, 2 = B, 35 = Ż).

Punkt kontrolny 10: Podstawowe najczęściej zadawane pytania o cyberbezpieczeństwo (Część A)

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

Q1: Czym jest złośliwe oprogramowanie?

Złośliwe oprogramowanie stworzone przez cyberprzestępców, aby uszkadzać urządzenia i sieci, przejmować nad nimi kontrolę lub kraść z nich dane.

Q2: Jaka jest różnica między wirusem a robakiem?

Wirus wymaga działania człowieka (np. otwarcia pliku), aby się rozprzestrzeniać, a robak rozprzestrzenia się automatycznie przez sieci.

Q3: Jak koń trojański infekuje komputer?

Oszukuje użytkowników, udając nieszkodliwy lub bezpieczny program i ukrywając w sobie złośliwy ładunek.

Q4: Czym jest ransomware?

Rodzaj złośliwego oprogramowania, które szyfruje pliki w systemie ofiary i żąda zapłaty w zamian za klucz deszyfrujący. [1]

Q5: Czym jest oprogramowanie szpiegujące (spyware)?

Złośliwe oprogramowanie, które potajemnie rejestruje naciśnięcia klawiszy, hasła i nawyki przeglądania użytkownika, aby wysyłać je atakującym.

Punkt kontrolny 10: Podstawowe najczęściej zadawane pytania o cyberbezpieczeństwo (Część B)

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

Q6: Co oznacza piaskownica (sandboxing)?

Uruchamianie podejrzanych plików w bezpiecznym, izolowanym środowisku wirtualnym w celu obserwowania ich zachowania bez ryzyka dla systemów produkcyjnych.

Q7: Czym jest złośliwe oprogramowanie bezplikowe (fileless malware)?

Złośliwe oprogramowanie działające bezpośrednio w pamięci systemowej (RAM) przy użyciu legalnych narzędzi, które nie zapisuje plików na dysku, aby ominąć podstawowe skanery.

Q8: Jak rootkit chroni złośliwe oprogramowanie?

Ukrywa złośliwe procesy i pliki, często przez podważenie jądra systemu operacyjnego, więc skanery antywirusowe mogą ich nie wykryć.

Q9: Czym jest dynamiczne monitorowanie zachowania?

Skanowanie antywirusowe, które w czasie rzeczywistym monitoruje aktywne procesy, aby blokować działania typowe dla złośliwego oprogramowania, takie jak masowe szyfrowanie plików.

Q10: Dlaczego powstrzymanie zagrożenia jest pilne podczas reagowania na incydent?

Izolowanie przejętych punktów końcowych zapobiega rozprzestrzenianiu się aktywnych ładunków złośliwego oprogramowania na inne urządzenia sieciowe.

Punkt kontrolny 10: Zaawansowane najczęściej zadawane pytania o bezpieczeństwo (Część C)

Poznaj zaawansowane aspekty techniczne ram bezpieczeństwa, analizy złośliwego oprogramowania i zgodności danych z przepisami.

Q1: Jak twórcy złośliwego oprogramowania omijają skanery antywirusowe oparte na sygnaturach?

Używają polimorfizmu, zmieniając skrót i strukturę kodu pliku przy każdej infekcji, przy zachowaniu tego samego złośliwego działania.

Q2: Jakie jest ryzyko narzędzi podwójnego zastosowania w kampaniach złośliwego oprogramowania?

Atakujący używają legalnych narzędzi administracyjnych (takich jak PowerShell lub Sysinternals), aby wtopić się w normalny ruch sieciowy, co utrudnia wykrycie.

Q3: Jak process hollowing uruchamia złośliwy ładunek?

Uruchamia legalny proces systemowy w stanie wstrzymanym, zastępuje jego kod w pamięci złośliwym oprogramowaniem i wznawia wykonanie.

Q4: Jaką rolę pełni serwer dowodzenia i kontroli (C2)?

Zdalny serwer obsługiwany przez hakerów, który wysyła instrukcje i ładunki do złośliwego oprogramowania działającego na zainfekowanych maszynach.

Q5: Dlaczego keylogging jest trudny do wykrycia?

Proste keyloggery zużywają minimalne zasoby procesora i ukrywają swoje procesy w legalnych narzędziach działających w przestrzeni użytkownika.

Punkt kontrolny 10: Zaawansowane najczęściej zadawane pytania o bezpieczeństwo (Część D)

Poznaj zaawansowane aspekty techniczne ram bezpieczeństwa, analizy złośliwego oprogramowania i zgodności danych z przepisami.

Q6: Jak obfuskacja kodu opóźnia analizę złośliwego oprogramowania?

Szyfruje lub przestawia kod źródłowy, czyniąc go nieczytelnym dla narzędzi analityków i skanerów bezpieczeństwa.

Q7: Jaką funkcję pełni bootkit?

Rootkit, który infekuje proces rozruchu (MBR, sektor rozruchowy lub oprogramowanie UEFI), więc uruchamia się przed załadowaniem systemu operacyjnego.

Q8: Jak skanowanie heurystyczne identyfikuje zagrożenia typu zero-day?

Skanuje podejrzane wzorce kodu i polecenia administracyjne zamiast szukać pasującego skrótu z bazy danych.

Q9: Jakie zagrożenie stanowi przejęcie DLL (DLL hijacking)?

Zmuszenie legalnej aplikacji do załadowania złośliwej dynamicznej biblioteki (DLL) przez umieszczenie jej w ścieżce katalogu aplikacji.

Q10: Jak zautomatyzowane potoki analizy złośliwego oprogramowania wykorzystują wirtualizację?

Uruchamiają podejrzane pliki na wielu maszynach wirtualnych z różnymi systemami, automatycznie generując logi zachowania i pliki PCAP ruchu sieciowego.

Część 11: 10 faktów o cyberbezpieczeństwie z praktyki i spostrzeżeń

Przejrzyj prawdziwe fakty dotyczące naruszeń bezpieczeństwa, mechanizmów obronnych i standardów zgodności.

1. WGLĄD W BEZPIECZEŃSTWO

Konie trojańskie pozostają częstą metodą infekcji, ponieważ ukrywają złośliwy kod w programach, które wyglądają niewinnie.

2. WGLĄD W BEZPIECZEŃSTWO

IC3 FBI otrzymało ponad 3 600 skarg dotyczących ransomware w 2025 r., a zgłoszone straty przekroczyły 32 miliony USD. [3]

3. WGLĄD W BEZPIECZEŃSTWO

Robaki mogą szybko rozprzestrzeniać się w sieciach, wykorzystując niezałatane luki w protokołach, takie jak EternalBlue w SMB.

4. WGLĄD W BEZPIECZEŃSTWO

Złośliwe oprogramowanie bezplikowe trudno wykryć, ponieważ działa w pamięci za pomocą legalnych narzędzi i pozostawia niewiele śladów na dysku.

5. WGLĄD W BEZPIECZEŃSTWO

Piaskownice analityczne zwykle wracają do czystej migawki po każdym uruchomieniu, dzięki czemu każdy test zaczyna się od znanego stanu.

6. WGLĄD W BEZPIECZEŃSTWO

Rootkity mogą modyfikować wywołania systemowe jądra, zgłaszając skanerom antymalware fałszywe wyniki diagnostyczne.

7. WGLĄD W BEZPIECZEŃSTWO

Obfuskacja kodu wykorzystuje narzędzia pakujące do kompresji i ukrycia prawdziwej struktury binarnego ładunku złośliwego oprogramowania.

8. WGLĄD W BEZPIECZEŃSTWO

Złośliwe oprogramowanie polimorficzne zmienia swój kod, a więc i skrót pliku, z każdą nową kopią, aby omijać kontrole sygnatur.

9. WGLĄD W BEZPIECZEŃSTWO

Przejęcie biblioteki DLL wykorzystuje konfiguracje kolejności wyszukiwania w standardowych systemach operacyjnych, takich jak Windows.

10. WGLĄD W BEZPIECZEŃSTWO

Dostawcy zabezpieczeń codziennie znajdują ogromne liczby nowych próbek złośliwego oprogramowania, więc sygnatury wymagają stałych aktualizacji.

Źródła i odnośniki techniczne

Przewodnik do nauki i interaktywne łamigłówki powstały na podstawie globalnych standardów NIST, OWASP i zgodności z przepisami o ochronie prywatności danych.

PUBLIKACJE NAUKOWE I BRANŻOWE

[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

Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

1 Pytanie 1

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Jaka jest cecha charakterystyczna konia trojańskiego? → Podszywa się pod legalne oprogramowanie, aby nakłonić użytkowników do jego uruchomienia

2 Pytanie 2

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Który typ złośliwego oprogramowania szyfruje pliki i żąda zapłaty? → Ransomware [1]

3 Pytanie 3

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Co reprezentuje oprogramowanie szpiegujące (spyware)? → Złośliwe oprogramowanie zaprojektowane do potajemnego monitorowania naciśnięć klawiszy i aktywności w przeglądarce

4 Pytanie 4

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Dlaczego twórcy złośliwego oprogramowania używają rootkitów? → Aby ukryć aktywne procesy i złośliwe pliki przed systemem operacyjnym

5 Pytanie 5

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Co oznacza sandboxing w analizie złośliwego oprogramowania? → Uruchamianie podejrzanych plików w izolowanym wirtualnym skarbcu, aby bezpiecznie obserwować ich zachowanie

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 Pytanie 6 — **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Fałsz: robaki same się powielają i rozprzestrzeniają w sieciach bez żadnego działania użytkownika.

7 Pytanie 7 — **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Fałsz: adware nie zawsze jest nieszkodliwe; wiele z niego śledzi przeglądanie, aby kierować reklamy.

8 Pytanie 8 — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Prawda: czyste kopie zapasowe offline przywracają zaszyfrowane pliki bez płacenia, choć skradzione dane mogą nadal wyciec.

9 Pytanie 9 — **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Fałsz: skanery sygnaturowe potrzebują znanej próbki, więc zupełnie nowe złośliwe oprogramowanie zero-day może się prześliznąć.

10 Pytanie 10 — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Złośliwe oprogramowanie bezplikowe wykonuje złośliwe skrypty w pamięci systemu, unikając zapisu plików na dysku.

Klucze słownictwa i kryteria oceny

Schemat oceniania dla nauczyciela: Przyznaj 1 punkt za każde poprawne dopasowanie (łącznie 8 pkt) i pojęcie w kontekście (łącznie 6 pkt).

PUNKT KONTROLNY 4: KLUCZ – DOPASOWYWANIE POJĘĆ

D 1. TROJAN	F 2. RANSOMWARE	A 3. OPROGRAMOWANIE SZPIEGUJĄCE	H 4. ROOTKIT
G 5. PIASKOWNICA	C 6. OGRANICZENIE	E 7. ROBAK KOMPUTEROWY	B 8. BEZPLIKOWE

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 TROJAN	2 RANSOMWARE	3 OPROGRAMOWANIE SZPIEGUJĄCE	4 ROOTKIT
5 PIASKOWNICA	6 IZOLOWANIE		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 D – ROOTKIT	2 F – IZOLOWANIE	3 H – BEZPLIKOWE	4 G – ROBAK
5 B – RANSOMWARE	6 C – SPYWARE	7 A – TROJAN	8 E – PIASKOWNICA

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia TROJAN, RANSOMWARE i OPROGRAMOWANIE SZPIEGUJĄCE oraz podać przykład każdego z nich.

Studia przypadków:
Poproś uczniów, aby uzasadniali swoje zalecenia faktami z karty pracy, a nie przypuszczeniami.

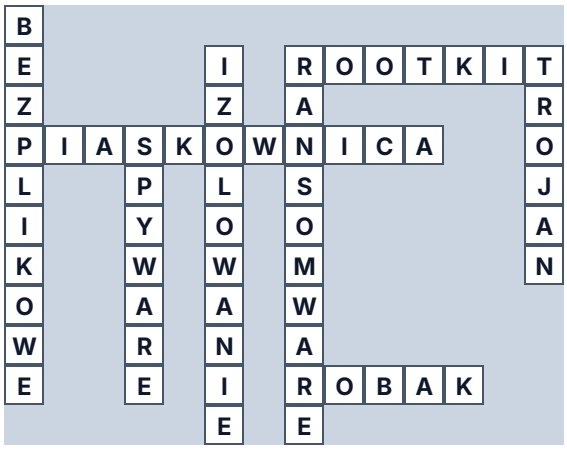
Ocena źródeł:
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

Klucze do łamigłówek i uwagi dla nauczyciela

ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

C	R	I	F	Ń	R	M	B	P	Y	P	O	C	U	S
Ś	E	Ł	J	B	A	B	E	C	Ó	R	Z	Ł	K	Z
E	L	Y	T	L	D	Q	Z	N	K	O	D	I	Ń	N
R	L	E	R	A	W	Y	P	S	Q	O	Ó	G	N	N
A	Q	R	S	T	P	T	L	F	B	T	Ś	P	I	O
W	H	S	B	W	I	Ć	I	Ś	Ź	K	V	C	Z	Ż
M	W	Ę	L	G	A	Ż	K	Ć	N	I	D	Q	O	Y
O	Ó	C	U	B	S	A	O	Ż	Ń	T	Ć	L	L	A
S	D	O	D	Ę	K	G	W	I	Ć	R	Q	N	O	M
N	E	I	S	Ż	O	R	E	Ś	Ę	Q	A	V	W	E
A	A	A	Q	Ó	W	O	N	P	T	J	Y	Q	A	K
R	R	T	S	Ć	N	B	N	Ź	O	B	Ę	S	N	Y
X	J	A	R	Ż	I	A	Z	R	Z	Ł	F	I	I	N
R	K	M	M	T	C	K	T	O	G	P	Q	G	E	Ż
Ą	O	V	F	V	A	B	Ź	S	Ź	B	G	M	Ż	G

ROZWIĄZANIE KRZYŻÓWKI



PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

3 poziomo: ROOTKIT Ukryte złośliwe oprogramowanie głęboko w jądrach systemów, utrzymujące kontrolę administracyjną. (7 liter)

5 poziomo: PIASKOWNICA Odizolowane środowisko wirtualne służące do bezpiecznej analizy złośliwych plików. (11 liter)

7 poziomo: ROBAK Samoreplikujące się złośliwe oprogramowanie rozprzestrzeniające się w sieciach bez udziału człowieka. (5 liter)

PIONOWO

1 pionowo: BEZPLIKOWE Złośliwe oprogramowanie wykonywane bezpośrednio w pamięci RAM, aby uniknąć wykrycia przez skanery dysków. (10 liter)

2 pionowo: IZOLOWANIE Ograniczanie zainfekowanych punktów końcowych, aby zapobiec rozprzestrzenianiu się ładunków zagrożeń. (10 liter)

3 pionowo: RANSOMWARE Złośliwe oprogramowanie szyfrujące pamięć masową systemu i żądające zapłaty za dostarczenie klucza. (10 liter)

4 pionowo: TROJAN Złośliwe oprogramowanie podszywające się pod nieszkodliwy lub użyteczny program narzędziowy. (6 liter)

6 pionowo: SPYWARE Program zaprojektowany do potajemnego monitorowania i rejestrowania aktywności oraz wprowadzanych danych użytkownika. (7 liter)

Klucz do słów rozsypanych i rozwiązania szyfru

Klucz odpowiedzi do ćwiczenia z rozszyfrowywania słownictwa i Tajemniczego wyzwania szyfrowego.

KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. OTJANR — **TROJAN**
2. SYERAWP — **SPYWARE**
3. PWONAICAKIS — **PIASKOWNICA**
4. BKARO — **ROBAK**
5. AMEASWORRN — **RANSOMWARE**
6. IOKRTTO — **ROOTKIT**
7. ZLIAWNIEOO — **IZOLOWANIE**
8. WPIEBLEKOZ — **BEZPLIKOWE**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"WYKRYWAJ ŁADUNKI ENDPOINT MONITOREM ZACHOWAŃ"

Klucz odpowiedzi do studiów przypadków

A Studium przypadku 1: Ograniczanie ładunku ransomware w firmie

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Firmowa sieć lokalna została naruszona przez aktywny ransomware. Kluczowe serwery plików zaczęły wyświetlać pliki z rozszerzeniem .locked. Ustal zasady powstrzymania ataku.
- Zalecana strategia i rozwiązanie: Odłącz wszystkie zaatakowane serwery od sieci lokalnej. Zakończ aktywne sesje administracyjne. Przywróć niezainfekowane pliki z bezpiecznego, zablokowanego do zapisu systemu kopii zapasowych offline.

B Studium przypadku 2: Bezplikowe złośliwe oprogramowanie wstrzykiwane do pamięci

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Analityk wykrywa podejrzane wzorce skryptów wykonywanych bezpośrednio w ulotnej pamięci RAM systemu za pomocą standardowych narzędzi administracyjnych, ale na dysku nie ma żadnych złośliwych plików.
- Zalecana strategia i rozwiązanie: Odizoluj zaatakowane punkty końcowe i najpierw zrób obraz pamięci. Przejrzyj logi PowerShell i WMI, zablokuj niezatwierdzone skrypty za pomocą AppLocker, a następnie uruchom ponownie system, aby usunąć ładunek.