Jméno: _____ Datum: _____ Body: _____

Analýza malwaru a zmírňování hrozeb Průvodce

Trojské koně, ransomware, spyware, rootkity, virtualizační sandboxy, izolace

ANALÝZA MALWARU – PŘEHLED UČIVA

ZABEZPEČENO

ŠIFROVÁNÍ DAT

Standard 256bitového AES

VYHOVUJÍCÍ

GLOBÁLNÍ STANDARDY

Rámce GDPR a CCPA

ZERO-TRUST

ZÁSADY PŘÍSTUPU

Vícefaktorové ověřování

Vítejte! Tento balíček aktivit vás provede analýzou a prevencí malwaru. Prozkoumáte spyware, trojské koně, ransomwarové payloady, nástroje reverzního inženýrství, chování rootkitů a strategie izolace.

KONTROLNÍ BODY PRACOVNÍHO LISTU

- [ ] **Část 1-4: Zvládněte kyberbezpečnost a prevenci hrozeb.**
- [ ] **Část 5-7: Vyřešte křížovku a osmisměrku.**
- [ ] **Část 8-9: Vyřešte případové studie a šifrovací výzvu.**
- [ ] **Část 10: Projděte si stránky se základními i pokročilými FAQ.**
- [ ] **Část 11: Prozkoumejte 10 zajímavých faktů z praxe.**
- [ ] **Bonus: výzva Mysli rychle.**

Otevřete průvodce kyberbezpečností od VPN.com

URL: https://www.vpn.com/cs/kyberneticka-bezpecnost/malware/

Váš studijní plán: zvládání malwaru

- Rozlište typy malwaru: trojský kůň, červ a rootkit.
- Zavést virtualizované sandboxové spouštění pro analýzu kódu.
- Navrhněte plány izolace a sanace aktivních ransomwarových payloadů.

PRŮVODCE ANALÝZOU MALWARU – POKYNY

Odpovězte na otázky s výběrem odpovědí a otázky pravda/nepravda, doplňte věty s vynechanými slovy pomocí banky slov, přiřaďte definice a vyřešte křížovku a osmisměrku. Uplatněte své znalosti na zmírňování malwaru. Zakončete bonusovou aktivitou Mysli rychle.

ANALÝZA MALWARU A OMEZENÍ ŠÍŘENÍ HROZEB (ÚVOD)

Škodlivý kód, jako jsou trojské koně, červi a ransomware, představuje vysoce nebezpečnou hrozbu pro koncová zařízení i servery. Bezpečnostní týmy analyzují malware ve virtuálních sandboxech a provádějí rychlou izolaci sítě, aby zabránily šíření škodlivého kódu.

PŘEČTĚTE SI POZORNĚ KAŽDÝ KONTROLNÍ BOD A VYBERTE NEBO NAPIŠTE SPRÁVNOU ODPOVĚĎ.

Kontrolní bod 1: Výzva s výběrem odpovědí

1. **1. Jaká je určující vlastnost trojského koně?**
   - A. Vydává se za legitimní software, aby přiměl uživatele ke spuštění
   - B. Replikuje se automaticky po místních síťových linkách
   - C. Infikuje soubory uvnitř izolovaných virtuálních sandboxů
   - D. Zachytává provoz poskytovatele internetu

2. **2. Jaký typ malwaru šifruje soubory a požaduje platbu?**
   - A. Ransomware
   - B. Spyware
   - C. Rootkit
   - D. Adware

3. **3. Co představuje spyware?**
   - A. Malware navržený k tajnému sledování stisků kláves a aktivit prohlížeče uživatele
   - B. Programový kód spouštěný uvnitř sandboxovaného virtuálního kontejneru
   - C. Antimalwarové aktualizace stahované z databázových registrů
   - D. Automatická úprava jasu obrazovky

4. **4. Proč vývojáři malwaru používají rootkity?**
   - A. Skrýt aktivní procesy a škodlivé soubory před operačním systémem
   - B. Zvýšit rychlost zpracování CPU na koncových bodech
   - C. Zálohovat databázové soubory do zabezpečených cloudových trezorů
   - D. Zlepšit výdrž baterie notebooků

5. **5. Co znamená sandboxing v analýze malwaru?**
   - A. Spouštění podezřelých souborů v izolovaném virtuálním trezoru k bezpečnému pozorování chování
   - B. Porovnávání hashů souborů se známými databázemi hrozeb
   - C. Obnovení záloh databáze po průniku
   - D. Odpojení místních síťových routerů od veřejných linek

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Počítačoví červi vyžadují k šíření po místních sítích interakci lidského uživatele.

- ◯ Pravda
- ◯ Nepravda

7 Otázka 7

7. Adware je vždy neškodný a nesleduje chování uživatele ani historii prohlížeče.

- ◯ Pravda
- ◯ Nepravda

8 Otázka 8

8. Obnovení čistých offline záloh umožňuje obětem obnovit zašifrované soubory bez placení výkupného.

- ◯ Pravda
- ◯ Nepravda

9 Otázka 9

9. Antivirus založený na signaturách spolehlivě zastaví zero-day malware dříve, než pro něj jakákoli signatura existuje.

- ◯ Pravda
- ◯ Nepravda

10 Otázka 10

10. Bezsouborový malware spouští škodlivé skripty v systémové paměti a vyhýbá se zápisu souborů na disk.

- ◯ Pravda
- ◯ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

Přečtěte si každou větu níže a doplňte do vynechaného místa správný termín ze slovní banky.

1. Malware maskovaný jako neškodný program se nazývá _____ .
2. Škodlivý kód, který za výkupné zamyká databázové systémy, se nazývá _____ .
3. Keylogger, který tajně zaznamenává hesla, patří do kategorie zvané _____ .
4. Hluboko v jádře operačního systému se dokáže skrýt _____ .
5. Podezřelé soubory se analyzují v izolovaném prostředí zvaném virtuální _____ .
6. K zastavení šíření aktivního škodlivého kódu je nutné okamžité síťové _____ .

ZÁSOBNÍK SLOV

BEZSOUBOROVÝ | ČERV | RANSOMWARE | ROOTKIT | SANDBOX | SPYWARE | TROJSKÝ KŮŇ | ZADRŽENÍ

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování bezpečnostních pojmů

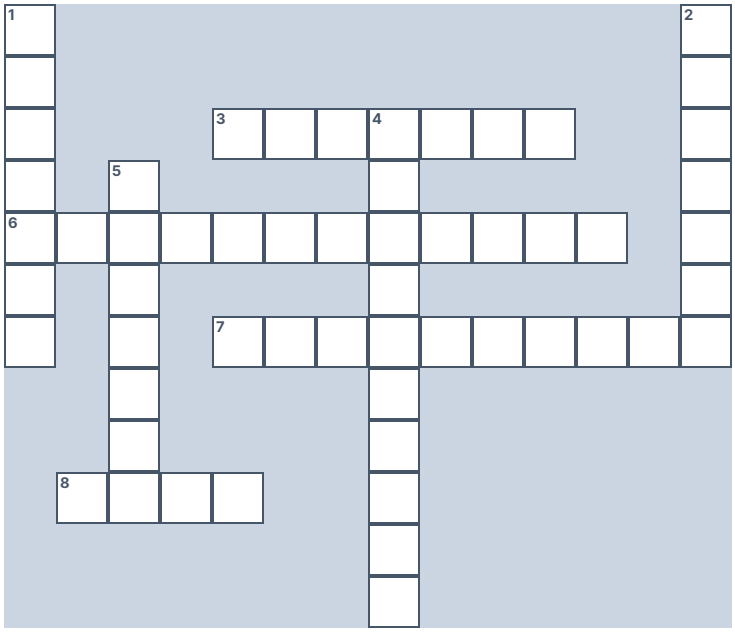
PŘIŘAZOVÁNÍ DEFINIC

Přiřaďte každý slovníčkový pojem vlevo k jeho správné definici vpravo zapsáním odpovídajícího písmene (A–H) do vyplnitelného pole.

☐	1. TROJSKÝ KŮŇ	A	Program navržený k tajnému sledování a zaznamenávání aktivity a vstupů uživatele.
☐	2. RANSOMWARE	B	Malware běžící přímo v RAM, aby unikl detekci diskovými skenery.
☐	3. SPYWARE	C	Omezení infikovaných koncových bodů, aby se zabránilo šíření škodlivého payloadu.
☐	4. ROOTKIT	D	Škodlivý software maskovaný jako neškodný nebo užitečný program.
☐	5. SANDBOX	E	Sebereplikující se malware šířící se po sítích bez lidského zásahu.
☐	6. ZADRŽENÍ	F	Malware, který šifruje systémové úložiště a požaduje platbu za vydání klíče.
☐	7. ČERV	G	Izolované virtuální prostředí používané k bezpečné analýze škodlivých souborů.
☐	8. BEZSOUBOROVÝ	H	Skrytý malware ukrývající se hluboko v jádrech systému, aby si udržel administrátorskou kontrolu.

Kontrolní bod 5: Křížovka

Vyřešte křížovku zapisováním písmen do aktivních bílých políček. Čísla odpovídají nápovědám níže.



VODOROVNÉ NÁPOVĚDY

3. Skrytý malware ukrytý hluboko v jádře systému k udržení administrátorské kontroly. (7)

6. Malware běžící přímo v RAM, aby unikl detekci diskovými skenery. (12)

7. Malware šifrující úložiště systému a požadující platbu za vydání klíče. (10)

8. Sebereplikující se malware šířící se sítěmi bez lidského zásahu. (4)

SVISLÉ NÁPOVĚDY

1. Izolované virtuální prostředí k bezpečné analýze škodlivých souborů. (7)

2. Program určený k tajnému sledování a záznamu aktivity a vstupů uživatele. (7)

4. Škodlivý software maskovaný jako neškodný nebo užitečný program. (10)

5. Omezení nakažených koncových bodů proti šíření škodlivých payloadů. (7)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

Uživatelé čteček obrazovky a klávesnice mohou odpovědi křížovky zapisovat přímo do textových polí níže.

VODOROVNÉ NÁPOVĚDY

3 vodorovně: Skrytý malware ukrytý hluboko v jádře systému k udržení administrátorské kontroly. (7 písmen):

6 vodorovně: Malware běžící přímo v RAM, aby unikl detekci diskovými skenery. (12 písmen):

7 vodorovně: Malware šifrující úložiště systému a požadující platbu za vydání klíče. (10 písmen):

8 vodorovně: Sebereplikující se malware šířící se sítěmi bez lidského zásahu. (4 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Izolované virtuální prostředí k bezpečné analýze škodlivých souborů. (7 písmen):

2 svisle: Program určený k tajnému sledování a záznamu aktivity a vstupů uživatele. (7 písmen):

4 svisle: Škodlivý software maskovaný jako neškodný nebo užitečný program. (10 písmen):

5 svisle: Omezení nakažených koncových bodů proti šíření škodlivých payloadů. (7 písmen):

Kontrolní bod 6: Hledání skrytých slov

Najděte 8 klíčových pojmů skrytých v mřížce níže. Slova mohou být vodorovně, svisle nebo úhlopříčně.

B	A	B	C	P	Y	L	R	E	J	Y	L	Y	U	K
Ď	Ř	N	J	D	I	O	O	R	Ň	S	K	R	Q	F
Ň	E	Ň	Ň	Ř	S	T	O	A	U	A	Ť	F	C	T
Ů	C	R	Ó	H	Š	B	T	W	V	N	D	T	Z	Ů
K	A	C	Ž	V	Ě	K	K	Y	G	D	Ž	D	R	Ň
Ý	L	Ď	Ř	X	Q	C	I	P	Ú	B	B	A	A	Ž
K	O	O	D	L	Č	A	T	S	Ď	O	Ó	Ď	N	É
S	Z	G	I	D	E	S	Ř	N	E	X	I	Š	S	Ž
J	I	T	É	Ř	R	Ů	E	A	Á	Ř	P	O	O	Q
O	U	Y	R	J	V	S	U	Š	Č	Ň	Ý	B	M	Ě
R	B	E	Z	S	O	U	B	O	R	O	V	Ý	W	Š
T	X	W	Í	A	S	Ž	Ý	Ý	L	F	I	N	A	S
J	N	M	Ť	P	G	R	Ř	G	Ž	Á	Ó	Ů	R	Ě
Ú	C	Ý	Š	Ý	B	G	M	Ž	F	J	Ó	Q	E	O
X	C	N	Ž	Z	Ě	Ý	P	W	Ú	L	Ů	Q	B	Ó

SEZNAM SLOV

TROJSKÝKŮŇ RANSOMWARE SPYWARE ROOTKIT SANDBOX IZOLACE ČERV BEZSOUBOROVÝ

Kontrolní bod 6, alternativa: Přístupné přiřazování slovíček

Přiřaďte každý z 8 slovníčkových pojmů z osmisměrky k jeho správné definici zapsáním písmene (A–H) do prázdného pole.

POJMY SLOVNÍ ZÁSOBY

- **A. TROJSKÝKŮŇ**
- **B. RANSOMWARE**
- **C. SPYWARE**
- **D. ROOTKIT**
- **E. SANDBOX**
- **F. IZOLACE**
- **G. ČERV**
- **H. BEZSOUBOROVÝ**

DEFINICE A POLE K PŘIŘAZENÍ

1. Skrytý malware ukrytý hluboko v jádře systému k udržení administrátorské kontroly.
2. Omezení nakažených koncových bodů proti šíření škodlivých payloadů.
3. Malware běžící přímo v RAM, aby unikl detekci diskovými skenery.
4. Sebereplikující se malware šířící se sítěmi bez lidského zásahu.
5. Malware šifrující úložiště systému a požadující platbu za vydání klíče.
6. Program určený k tajnému sledování a záznamu aktivity a vstupů uživatele.
7. Škodlivý software maskovaný jako neškodný nebo užitečný program.
8. Izolované virtuální prostředí k bezpečné analýze škodlivých souborů.

Kontrolní bod 7: Výzva s přeházenými slovy

Přeuspořádejte písmena níže a odhalte klíčové pojmy a termíny kybernetické bezpečnosti. Odpovědi pište do připravených polí.

1. **ŮÝKSRTKŇJO**
2. **SYERAWP**
3. **DSBXNOA**
4. **VRČE**
5. **AMEASWORRN**
6. **IOKRTTO**
7. **ICAEZLO**
8. **OZOOBÝBUEVRS**

Bonusová aktivita: Mysli rychle

3 ODPOVĚDI V KAŽDÉ KATEGORII. VYHRÁVÁ, KDO PRVNÍ VYPLNÍ CELÝ SEZNAM.

1	Místa, kde stahovat bezpečné aplikace			
2	Zařízení, která lze hacknout			
3	Věci, které si zálohujete			
4	Varovné signály v e-mailu			
5	Známky, že je v telefonu malware			
6	Typy malwaru, které znáte			
7	Typy souborů, u kterých je třeba opatrnosti			
8	Způsoby, jak se malware dostane do počítače			
9	Bezpečné návyky, se kterými můžete začít už dnes			
10	Slova související s kyberbezpečností			
11	Co udělat po úniku dat			
12	Důvody, proč aktualizovat software			
13	Zvířata nebo postavy s názvy podobnými malwaru			
14	Věci, které může malware ukrást			
15	Věci, které je třeba udělat, když kliknete na špatný odkaz			

Kontrolní bod 8: Případové studie kyberbezpečnosti

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: ZADRŽENÍ RANSOMWAROVÉHO PAYLOADU V PODNIKU



Scénář: Firemní lokální síť byla napadena aktivním ransomwarem. Klíčové souborové servery začaly zobrazovat přípony souborů s .locked. Stanovte zásady zamezení šíření.

Otázka k diskusi: Popište kroky izolace a nastíněte protokol obnovy dat.

PŘÍPADOVÁ STUDIE 2: PAMĚŤOVÁ INJEKCE BEZSOUBOROVÉHO MALWARU



Scénář: Analytik odhalí podezřelé skriptovací vzorce spouštěné pomocí standardních administrativních nástrojů přímo ve volatilní systémové RAM, ale na disku žádné škodlivé soubory nejsou.

Otázka k diskusi: Vysvětlete strategii analýzy paměti a určete nástroje k blokování bezsouborového spouštění.

Kontrolní bod 9: Dešifrování šifry

Profesionál v kyberbezpečnosti chrání síťová aktiva před online útočníky. Pomocí níže uvedeného klíče písmeno–číslo dešifrujte zprávu zapsáním odpovídajících písmen do prázdných polí.

ŠIFROVACÍ KLÍČ PÍSMENO–ČÍSLO

A=1 Á=2 B=3 C=4 Č=5 D=6 Ď=7 E=8 É=9 Ě=10 F=11 G=12 H=13 I=14
Í=15 J=16 K=17 L=18 M=19 N=20 Ň=21 O=22 Ó=23 P=24 Q=25 R=26 Ř=27 S=28
Š=29 T=30 Ť=31 U=32 Ú=33 Ů=34 V=35 W=36 X=37 Y=38 Ý=39 Z=40 Ž=41

6	8	30	8	17	32	16	30	8		13	26	22	40	3	38

3	8	13	1	35	14	22	26	2	18	20	15	19	14

19	22	20	14	30	22	26	38

Dešifrovaná zpráva:

TIP: KAŽDÉ ČÍSLO PŘEDSTAVUJE POZICI DANÉHO PÍSMENE V ABECEDĚ (NAPŘ. 1 = A, 2 = B, 41 = Ž).

Kontrolní bod 10: Základní časté otázky ke kyberbezpečnosti (část A)

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q1: Co je malware?

Škodlivý software vytvořený útočníky k poškození, ovládnutí nebo krádeži dat ze zařízení a sítí.

Q2: Jaký je rozdíl mezi virem a červem?

Virus ke svému šíření vyžaduje lidskou akci (například otevření souboru), zatímco červ se šíří sítěmi automaticky.

Q3: Jak trojský kůň infikuje počítač?

Klame uživatele tím, že se vydává za neškodný nebo bezpečný program a skrývá v sobě škodlivý obsah.

Q4: Co je ransomware?

Typ malwaru, který šifruje soubory v cílovém systému a požaduje finanční platbu výměnou za dešifrovací klíč. [1]

Q5: Co je spyware?

Škodlivý software, který tajně zaznamenává stisky kláves, hesla a návyky při prohlížení a odesílá je útočníkům.

Kontrolní bod 10: Základní časté otázky ke kyberbezpečnosti (část B)

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q6: Co znamená sandboxing?

Spouštění podezřelých souborů v zabezpečeném izolovaném virtuálním prostředí k pozorování jejich chování bez rizika pro produkční systémy.

Q7: Co je bezsouborový malware?

Malware, který běží přímo v systémové paměti (RAM) pomocí legitimních nástrojů a vyhýbá se zápisu souborů na disk, aby obešel základní skenery.

Q8: Jak rootkit chrání malware?

Skrývá škodlivé procesy a soubory, často podvracením jádra operačního systému, takže je antivirové skenery mohou přehlédnout.

Q9: Co je dynamické monitorování chování?

Antivirové skenování, které v reálném čase monitoruje aktivní procesy a blokuje akce typické pro malware, jako je hromadné šifrování souborů.

Q10: Proč je izolace během reakce na incident naléhavá?

Izolace kompromitovaných koncových bodů brání aktivnímu malwaru v šíření na další síťová zařízení.

Kontrolní bod 10: Pokročilé časté otázky k bezpečnosti (část C)

Prozkoumejte pokročilé technické aspekty bezpečnostních rámců, analýzy malwaru a datové compliance.

Q1: Jak vývojáři malwaru obcházejí antivirové skenery založené na signaturách?

Používají polymorfismus: s každou infekcí mění hash a strukturu kódu souboru, zatímco škodlivé chování zůstává stejné.

Q2: Jaké je riziko nástrojů dvojího užití v malwarových kampaních?

Útočníci používají legitimní administrátorské nástroje (jako PowerShell nebo Sysinternals), aby splynuli s běžným síťovým provozem, což ztěžuje detekci.

Q3: Jak process hollowing spouští škodlivý kód?

Spustí legitimní systémový proces v pozastaveném stavu, nahradí jeho kód v paměti malwarem a obnoví běh.

Q4: Jaká je role Command and Control (C2) serveru?

Vzdálený server provozovaný hackery k odesílání pokynů a škodlivého obsahu malwaru běžícímu na kompromitovaných strojích.

Q5: Proč je keylogging obtížně odhalitelný?

Základní keyloggery spotřebovávají minimální prostředky CPU a skrývají své procesy v legitimních nástrojích uživatelského prostoru.

Kontrolní bod 10: Pokročilé časté otázky k bezpečnosti (část D)

Prozkoumejte pokročilé technické aspekty bezpečnostních rámců, analýzy malwaru a datové compliance.

Q6: Jak obfuskace kódu zdržuje analýzu malwaru?

Šifruje nebo přeskupuje zdrojový kód, čímž jej činí nečitelným pro analytické nástroje a bezpečnostní skenery.

Q7: Jaká je funkce bootkitu?

Rootkit, který infikuje zaváděcí proces (MBR, zaváděcí sektor nebo firmware UEFI), takže se spouští před načtením operačního systému.

Q8: Jak heuristické skenování identifikuje zero-day hrozby?

Hledá podezřelé vzory kódu a administrátorské příkazy, místo aby hledal odpovídající haš v databázi.

Q9: Jaká je hrozba DLL hijackingu?

Donucení legitimní aplikace načíst škodlivou dynamicky linkovanou knihovnu (DLL) jejím umístěním do adresářové cesty aplikace.

Q10: Jak automatizované pipeline analýzy malwaru využívají virtualizaci?

Spouštějí podezřelé soubory ve virtuálních strojích s různými OS a automaticky generují logy chování a síťové soubory PCAP.

Část 11: 10 faktů a poznatků o kyberbezpečnosti z praxe

Projděte si fakta z praxe o bezpečnostních incidentech, obranných mechanismech a standardech souladu.

1. BEZPEČNOSTNÍ POSTŘEH

Trojské koně zůstávají běžnou metodou infekce, protože skrývají škodlivý kód v programech, které vypadají neškodně.

2. BEZPEČNOSTNÍ POSTŘEH

IC3 při FBI obdrželo v roce 2025 přes 3 600 stížností na ransomware, s nahlášenými ztrátami přesahujícími $32 milionů. [3]

3. BEZPEČNOSTNÍ POSTŘEH

Červi se mohou rychle šířit sítěmi zneužíváním neopravených zranitelností protokolů, jako byl EternalBlue v SMB.

4. BEZPEČNOSTNÍ POSTŘEH

Bezsouborový malware se těžko detekuje, protože běží v paměti prostřednictvím legitimních nástrojů a na disku zanechává jen málo stop.

5. BEZPEČNOSTNÍ POSTŘEH

Analytické sandboxy se po každém běhu obvykle vracejí k čistému snímku, takže každý test začíná ze známého stavu.

6. BEZPEČNOSTNÍ POSTŘEH

Rootkity dokážou upravit systémová volání jádra a hlásit antimalwarovým skenerům falešné diagnostické výsledky.

7. POSTŘEH K BEZPEČNOSTI

Obfuskace kódu využívá packery ke kompresi a skrytí skutečné binární struktury payloadu malwaru.

8. POSTŘEH K BEZPEČNOSTI

Polymorfní malware mění s každou novou kopií svůj kód, a tedy i hash souboru, aby unikl kontrolám signatur.

9. POSTŘEH K BEZPEČNOSTI

DLL hijacking zneužívá konfiguraci pořadí vyhledávání ve standardních operačních systémech, jako je Windows.

10. BEZPEČNOSTNÍ POSTŘEH

Bezpečnostní dodavatelé denně nacházejí obrovské množství nových vzorků malwaru, takže signatury vyžadují neustálé aktualizace.

Technické reference a zdroje

Studijní příručka a interaktivní hádanky jsou sestaveny z globálních standardů NIST, OWASP a předpisů o ochraně osobních údajů.

AKADEMICKÉ A OBOROVÉ REFERENCE

[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

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 **Otázka 1** — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Jaká je určující vlastnost trojského koně? → Vydává se za legitimní software, aby přiměl uživatele ke spuštění

2 **Otázka 2** — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Jaký typ malwaru šifruje soubory a požaduje platbu? → Ransomware [1]

3 **Otázka 3** — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Co představuje spyware? → Malware navržený k tajnému sledování stisků kláves a aktivit prohlížeče uživatele

4 **Otázka 4** — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Proč vývojáři malwaru používají rootkity? → Skrýt aktivní procesy a škodlivé soubory před operačním systémem

5 **Otázka 5** — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Co znamená sandboxing v analýze malwaru? → Spouštění podezřelých souborů v izolovaném virtuálním trezoru k bezpečnému pozorování chování

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 Otázka 6

Správná odpověď: Nepravda

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: červi se sami replikují a šíří po sítích bez jakékoli akce uživatele.

7 Otázka 7

Správná odpověď: Nepravda

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: adware není vždy neškodný; velká část sleduje prohlížení kvůli cílení reklam.

8 Otázka 8

Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Pravda: čisté offline zálohy obnoví zašifrované soubory bez placení, i když ukradená data mohou stále uniknout.

9 Otázka 9

Správná odpověď: Nepravda

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: signaturové skenery potřebují známý vzorek, takže zbrusu nový zero-day malware jim může proklouznout.

10 Otázka 10

Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Bezsouborový malware spouští škodlivé skripty v systémové paměti a vyhýbá se zápisu souborů na disk.

Klíče slovní zásoby a hodnoticí rubrika

Hodnoticí rubrika pro vyučující: Udělte 1 bod za každé správné přiřazení (celkem 8 bodů) a kontextový termín (celkem 6 bodů).

KONTROLNÍ BOD 4: KLÍČ K PŘIŘAZOVÁNÍ POJMŮ

D 1. TROJSKÝ KŮŇ	F 2. RANSOMWARE	A 3. SPYWARE	H 4. ROOTKIT
G 5. SANDBOX	C 6. ZADRŽENÍ	E 7. ČERV	B 8. BEZSOUBOROVÝ

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 TROJSKÝ KŮŇ	2 RANSOMWARE	3 SPYWARE	4 ROOTKIT
5 SANDBOX	6 ZADRŽENÍ		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 D – ROOTKIT	2 F – IZOLACE	3 H – BEZSOUBOROVÝ	4 G – ČERV
5 B – RANSOMWARE	6 C – SPYWARE	7 A – TROJSKÝKŮŇ	8 E – SANDBOX

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy TROJSKÝ KŮŇ, RANSOMWARE a SPYWARE a ke každému uvést příklad.

Případové studie:
Požádejte studenty, aby svá doporučení zdůvodnili fakty z pracovního listu, nikoli domněnkami.

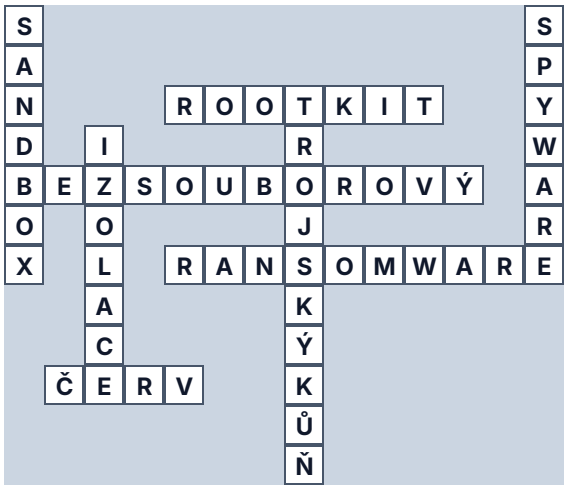
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

B	A	B	C	P	Y	L	R	E	J	Y	L	Y	U	K
Ď	Ř	N	J	D	I	O	O	R	Ň	S	K	R	Q	F
Ň	E	Ň	Ň	Ř	S	T	O	A	U	A	Ť	F	C	T
Ů	C	R	Ó	H	Š	B	T	W	V	N	D	T	Z	Ů
K	A	C	Ž	V	Ě	K	K	Y	G	D	Ž	D	R	Ň
Ý	L	Ď	Ř	X	Q	C	I	P	Ú	B	B	A	A	Ž
K	O	O	D	L	Č	A	T	S	Ď	O	Ó	Ď	N	É
S	Z	G	I	D	E	S	Ř	N	E	X	I	Š	S	Ž
J	I	T	É	Ř	R	Ů	E	A	Á	Ř	P	O	O	Q
O	U	Y	R	J	V	S	U	Š	Č	Ň	Ý	B	M	Ě
R	B	E	Z	S	O	U	B	O	R	O	V	Ý	W	Š
T	X	W	Í	A	S	Ž	Ý	Ý	L	F	I	N	A	S
J	N	M	Ť	P	G	R	Ř	G	Ž	Á	Ó	Ů	R	Ě
Ú	C	Ý	Š	Ý	B	G	M	Ž	F	J	Ó	Q	E	O
X	C	N	Ž	Z	Ě	Ý	P	W	Ú	L	Ů	Q	B	Ó

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

3 vodorovně: ROOTKIT Skrytý malware ukrytý hluboko v jádře systému k udržení administrátorské kontroly. (7 písmen)

6 vodorovně: BEZSOUBOROVÝ Malware běžící přímo v RAM, aby unikl detekci diskovými skenery. (12 písmen)

7 vodorovně: RANSOMWARE Malware šifrující úložiště systému a požadující platbu za vydání klíče. (10 písmen)

8 vodorovně: ČERV Sebereplikující se malware šířící se sítěmi bez lidského zásahu. (4 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: SANDBOX Izolované virtuální prostředí k bezpečné analýze škodlivých souborů. (7 písmen)

2 svisle: SPYWARE Program určený k tajnému sledování a záznamu aktivity a vstupů uživatele. (7 písmen)

4 svisle: TROJSKÝKŮŇ Škodlivý software maskovaný jako neškodný nebo užitečný program. (10 písmen)

5 svisle: IZOLACE Omezení nakažených koncových bodů proti šíření škodlivých payloadů. (7 písmen)

Klíč řešení přesmyček a šifry

Klíč k hodnocení aktivity s přesmyčkami slovní zásoby a výzvy Tajná šifra.

KLÍČ K PŘESMYČKÁM

1.	ŮÝKSRTKŇJO	TROJSKÝKŮŇ	5.	AMEASWORRN	RANSOMWARE
2.	SYERAWP	SPYWARE	6.	IOKRTTO	ROOTKIT
3.	DSBXNOA	SANDBOX	7.	ICAEZLO	IZOLACE
4.	VRČE	ČERV	8.	OZOOBÝBUEVRS	BEZSOUBOROVÝ

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"DETEKUJTE HROZBY BEHAVIORÁLNÍMI MONITORY"

Klíč k případovým studiím

A Případová studie 1: Zadržení ransomwarového payloadu v podniku

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Firemní lokální síť byla napadena aktivním ransomwarem. Na klíčových souborových serverech se začaly objevovat soubory s příponou .locked. Stanovte zásady izolace nákazy.
- Doporučená strategie a řešení: Odpojte všechny zasažené servery od lokální sítě. Ukončete aktivní administrátorské relace. Obnovte nekompromitované soubory ze zabezpečeného offline zálohovacího systému chráněného proti zápisu.

B Případová studie 2: Paměťová injekce bezsouborového malwaru

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Analytik detekuje podezřelé skriptovací vzorce spouštěné přímo ve volatilní systémové RAM pomocí standardních administrátorských nástrojů, ale na disku žádné škodlivé soubory neexistují.
- Doporučená strategie a řešení: Izolujte postižené koncové body a nejprve pořiďte obraz paměti. Projděte logy PowerShellu a WMI, zablokujte neschválené skripty pomocí AppLockeru a poté restartujte, aby se payload vymazal.