Nafn: _____ Dagsetning: _____ Stig: _____

Greining spilliforrita og viðbrögð við ógnum
Leiðarvísir

Trójuhestar, kúgunarhugbúnaður, njósnaforrit, rótarsett, sýndarvæðingarsandkassar, einangrun

YFIRLIT UM GREININGU SPILLIFORRITA

VARIÐ
GAGNADULKÓÐUN
256-bita AES staðall

UPPFYLLIR KRÖFUR
ALÞJÓÐLEGIR STAÐLAR
Rammar GDPR og CCPA

ZERO-TRUST
AÐGANGSSTEFNA
Fjölþátta auðkenning

Velkomin! Þetta verkefnahefti leiðir þig í gegnum greiningu og forvarnir gegn spilliforritum. Þú munt kynnast njósnaforritum, trójuhestum, gíslatökuforritum, tólum til bakverkfræði, hegðun rótarpakka og aðferðum til að halda smiti í skefjum.

ÁFANGAR VERKEFNABLAÐSINS

- [ ] **Hluti 1-4: Náðu tökum á netöryggi og varnir gegn ógnum.**
- [ ] **Hluti 5-7: Leystu krossgátur og orðaleitarþrautir.**
- [ ] **Hluti 8-9: Leystu dæmisögur og dulmálsáskorun.**
- [ ] **Hluti 10: Farðu yfir síður með algengum spurningum, grunnstig og framhaldsstig.**
- [ ] **Hluti 11: Kannaðu 10 áhugaverðar staðreyndir úr raunheimum.**
- [ ] **Auka: áskorunin Hugsaðu hratt.**

Opnaðu netöryggisleiðarvísi VPN.com

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

Námsvegvísir þinn: varnir gegn spilliforritum

- Gerðu greinarmun á Trójuhesti, ormi og rótarsetu sem tegundum spilliforrits.
- Innleiddu keyrslu í einangruðu sýndarumhverfi (sandbox) fyrir kóðagreiningu.
- Hannaðu áætlanir um einangrun og hreinsun virks gíslatökuhugbúnaðar.

LEIÐBEININGAR UM GREININGU SPILLIFORRITA

Svaraðu fjölvalsspurningunum og satt/ósatt-spurningunum, kláraðu eyðufyllingarsetningarnar með orðabankanum, paraðu saman skilgreiningar og leystu krossgátuna og orðaleitina. Nýttu þekkingu þína á að draga úr áhrifum spilliforrita. Ljúktu með aukaverkefninu Hugsaðu hratt.

GREINING SPILLIFORRITA OG INNILOKUN ÓGNA (INNGANGUR)

Skaðlegur kóði eins og Trójuhestar, ormar og gíslatökuforrit ógnar endabúnaði og netþjónum alvarlega. Öryggisteymi greina spilliforrit í sýndarsandkössum og grípa hratt til netaðskilnaðar til að takmarka útbreiðslu skaðlegs farms.

LESTU HVERN ÁFANGA VANDLEGA OG VELDU EÐA SKRIFAÐU RÉTT SVAR.

Áfangi 1: Fjölvalsáskorun

1 **1. Hvað einkennir tróverja (Trojan horse)?**

- A. Það þykist vera lögmætur hugbúnaður til að blekkja notendur til að keyra það
- B. Það dreifir sér sjálfkrafa um staðarnetið
- C. Það smitar skrár í einangruðum sýndarsandkössum
- D. Það hlerar umferð netþjónustuveitu

2 **2. Hvaða gerð spilliforrits dulkóðar skrár og krefst greiðslu?**

- A. Kúgunarhugbúnaður
- B. Njósnaforrit
- C. Rótarsett (rootkit)
- D. Auglýsingaforrit (adware)

3 **3. Hvað táknar njósnahugbúnaður?**

- A. Spilliforrit sem er hannað til að fylgjast leynilega með lyklaborðsslögum og vafravirkni notenda
- B. Forritskóði sem keyrir í sandkassa í sýndargámi
- C. Uppfærslur gegn spilliforritum sóttar úr gagnagrunnsskrám
- D. Sjálfvirk stilling á birtustigi skjás

4 **4. Hvers vegna nota höfundar spilliforrita rótarsett (rootkits)?**

- A. Til að fela virk ferli og skaðlegar skrár fyrir stýrikerfinu
- B. Til að auka vinnsluhraða örgjörva í endabúnaði
- C. Til að taka afrit af gagnagrunnsskrám í örugga skýjahvelfingu
- D. Til að bæta rafhlöðuendingu í fartölvum

5 **5. Hvað merkir sandkassi (sandboxing) í greiningu spilliforrita?**

- A. Að keyra grunsamlegar skrár í einangruðu sýndarhólfi til að fylgjast örugglega með hegðun þeirra
- B. Að skanna kjötkássur skráa gegn þekktum ógnagagnagrunnum
- C. Að endurheimta afrit gagnagrunna eftir innbrot
- D. Að aftengja staðarnetsbeina frá opinberum línum

Áfangi 2: Satt eða ósatt

6 Spurning 6

6. Netormar þurfa að notandi grípi inn í til að dreifa sér um staðarnet.

○ Satt ○ Ósatt

7 Spurning 7

7. Auglýsingahugbúnaður (adware) er alltaf skaðlaus og fylgist ekki með hegðun notenda eða vafrasögu.

○ Satt ○ Ósatt

8 Spurning 8

8. Með því að endurheimta hrein afrit án nettengingar geta fórnarlömb endurheimt dulkóðaðar skrár án þess að greiða lausnargjaldið.

○ Satt ○ Ósatt

9 Spurning 9

9. Vírusvörn byggð á undirskriftum stöðvar áreiðanlega núlldagsspilliforrit áður en undirskrift fyrir það er til.

○ Satt ○ Ósatt

10 Spurning 10

10. Skráarlaust spilliforrit keyrir skaðleg skriftur í kerfisminni og forðast að skrifa skrár á diskinn.

○ Satt ○ Ósatt

Áfangi 3: Lykilhugtök fyllt inn

Lestu hverja setningu hér að neðan og fylltu í eyðuna með réttu hugtaki úr orðabankanum.

1. Spilliforrit sem dulbýr sig sem öruggt gagnaforrit er _____ .

2. Skaðlegur farmur sem læsir gagnagrunnskerfum fyrir fé er dæmi um _____ .

3. Lyklaborðsnjósnarar sem taka leynilega upp lykilorð eru dæmi um _____ .

4. Til að fela sig djúpt í kjörnum stýrikerfa þarf _____ .

5. Til að greina grunsamlegar skrár í einangruðu hólfi er notað sýndarumhverfi sem kallast _____ .

6. Til að stöðva útbreiðslu virks skaðlegs farms spilliforrits þarf tafarlausa _____ á netinu.

ORÐABANKI

EINANGRUN NJÓSNAFORRIT ORMUR RANSOMWARE ROOTKIT SANDKASSI SKRÁARLAUST TRÓJUHESTUR

Skrifaðu svörin þín hér:

1. **2.**

3. **4.**

5. **6.**

Áfangi 4: Pörun hugtaka um öryggi

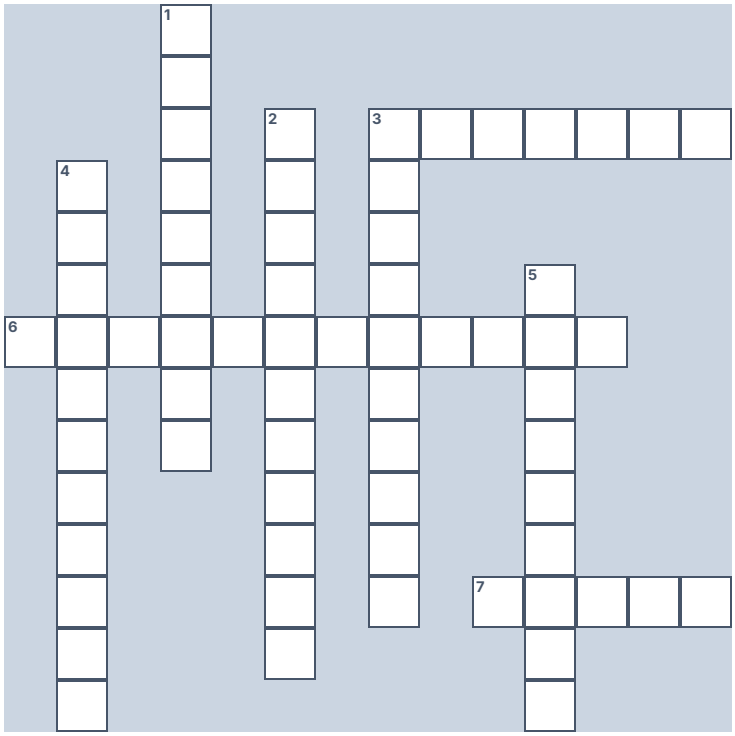
PÖRUN SKILGREININGA

Paraðu hvert hugtak til vinstri við rétta skilgreiningu til hægri með því að skrifa samsvarandi bókstaf (A-H) í útfyllanlega reitinn.

☐	1. TRÓJUHESTUR	A	Forrit hannað til að fylgjast með og skrá leynilega athafnir og innslátt notenda.
☐	2. GÍSLATÖKUFORRIT	B	Spilliforrit sem keyra beint í vinnsluminni til að komast hjá greiningu diskaskanna.
☐	3. NJÓSNAFORRIT	C	Að takmarka sýkta endapunkta til að koma í veg fyrir útbreiðslu skaðlegs farms.
☐	4. RÓTARSETT	D	Skaðlegur hugbúnaður dulbúinn sem meinlaust eða gagnlegt hjálparforrit.
☐	5. SANDKASSI	E	Sjálfafritandi spilliforrit sem dreifist um net án aðgerða manna.
☐	6. AFMÖRKUN	F	Spilliforrit sem dulkóðar geymslu kerfisins og krefst greiðslu fyrir afhendingu lykils.
☐	7. WORM	G	Einangrað sýndarumhverfi sem notað er til að greina skaðlegar skrár á öruggan hátt.
☐	8. SKRÁARLAUS	H	Falið spilliforrit djúpt í kerfiskjörnum sem viðheldur stjórnunarstjórn.

Áfangi 5: Krossgáta

Leystu krossgátuna með því að slá stafi inn í virku hvítu reitina. Tölurnar vísa til vísbendinganna hér að neðan.



LÁRÉTT

3. Spilliforrit sem felur sig djúpt í kjarna kerfisins til að halda stjórnandavöldum (7)

6. Forrit sem er hannað til að fylgjast leynilega með og skrá athafnir og innslátt notanda (12)

7. Sjálfafritandi spilliforrit sem dreifir sér um net án aðgerða manna (5)

LÓÐRÉTT

1. Einangrað sýndarumhverfi sem notað er til að greina skaðlegar skrár á öruggan hátt (9)

2. Spilliforrit sem keyrir beint í vinnsluminni til að komast hjá greiningu diskaskanna (11)

3. Spilliforrit sem dulkóðar geymslu kerfis og krefst greiðslu fyrir afhendingu lykils (10)

4. Skaðlegur hugbúnaður sem dulbýr sig sem meinlaust eða gagnlegt forrit (11)

5. Takmörkun á smituðum endapunktum til að koma í veg fyrir dreifingu skaðlegs farms (9)

Áfangi 5, valkostur: Aðgengilegar vísbendingar fyrir krossgátu

Notendur skjálesara og lyklaborðs geta slegið svör krossgátunnar beint inn í textareitina hér að neðan.

LÁRÉTT

3 lárétt: Spilliforrit sem felur sig djúpt í kjarna kerfisins til að halda stjórnandavöldum (7 stafir):

6 lárétt: Forrit sem er hannað til að fylgjast leynilega með og skrá athafnir og innslátt notanda (12 stafir):

7 lárétt: Sjálfafritandi spilliforrit sem dreifir sér um net án aðgerða manna (5 stafir):

LÓÐRÉTT

1 lóðrétt: Einangrað sýndarumhverfi sem notað er til að greina skaðlegar skrár á öruggan hátt (9 stafir):

2 lóðrétt: Spilliforrit sem keyrir beint í vinnsluminni til að komast hjá greiningu diskaskanna (11 stafir):

3 lóðrétt: Spilliforrit sem dulkóðar geymslu kerfis og krefst greiðslu fyrir afhendingu lykils (10 stafir):

4 lóðrétt: Skaðlegur hugbúnaður sem dulbýr sig sem meinlaust eða gagnlegt forrit (11 stafir):

5 lóðrétt: Takmörkun á smituðum endapunktum til að koma í veg fyrir dreifingu skaðlegs farms (9 stafir):

Áfangi 6: Falið orð í orðaleit

Finndu 8 lykilhugtök sem eru falin í reitnum hér að neðan. Orð geta verið lárétt, lóðrétt eða á ská.

A N Đ O Đ É G R I Đ S R M E I
R U T Ö U É R A X É S A A R Ó
U R R U M R O N N P A Ú Þ R J
T G S Ú T D N S Æ B N F T Ý Y
S N Í A S Ö Æ O Æ K D F I S M
E A S J L L U M Ó G K P R K G
H N Ö A O X F W V B A Æ T R Æ
U I Á G L Ö G A J O S P N Á Ý
J E B L Ö Æ F R Þ Ó S Y V A K
Ó V P Á O X Ú E L G I X D R Þ
R N J Ó S N A F O R R I T L V
T J S Á Ý Ö Þ M T R Ý I Ó A Đ
A D R O O T K I T J R Y Ý U Ý
K Í H Ú H F Á É I K U T Y S S
Ö E H É T D A L P B Ö M J T X

ORÐALISTI

TRÓJUHESTUR RANSOMWARE NJÓSNAFORRIT ROOTKIT SANDKASSI
EINANGRUN ORMUR SKRÁARLAUST

Áfangi 6, valkostur: Aðgengileg orðaforðapörun

Paraðu hvert af hugtökunum 8 úr orðaleitinni við rétta skilgreiningu með því að skrifa bókstafinn (A-H) í eyðuna.

HUGTÖK
A. TRÓJUHESTUR
B. RANSOMWARE
C. NJÓSNAFORRIT
D. ROOTKIT
E. SANDKASSI
F. EINANGRUN
G. ORMUR
H. SKRÁARLAUST

SKILGREININGAR OG PÖRUNARREITIR	
	1. Spilliforrit sem felur sig djúpt í kjarna kerfisins til að halda stjórnandavöldum.
	2. Takmörkun á smituðum endapunktum til að koma í veg fyrir dreifingu skaðlegs farms.
	3. Spilliforrit sem keyrir beint í vinnsluminni til að komast hjá greiningu diskaskanna.
	4. Sjálfafritandi spilliforrit sem dreifir sér um net án aðgerða manna.
	5. Spilliforrit sem dulkóðar geymslu kerfis og krefst greiðslu fyrir afhendingu lykils.
	6. Forrit sem er hannað til að fylgjast leynilega með og skrá athafnir og innslátt notanda.
	7. Skaðlegur hugbúnaður sem dulbýr sig sem meinlaust eða gagnlegt forrit.
	8. Einangrað sýndarumhverfi sem notað er til að greina skaðlegar skrár á öruggan hátt.

Áfangi 7: Áskorun með ruglaðum orðum

Raðaðu stöfunum hér að neðan í rétta röð til að afhjúpa lykilhugtök um netöryggi. Skrifaðu svörin þín í reitina sem fylgja.

1. UEURHSTTÓRJ
2. TJNANRIÓORFS
3. SAKASIDSN
4. MRUOR
5. AMEASWORRN
6. IOKRTTO
7. GEUNRAINN
8. ULTRRSAKSAÁ

Aukaverkefni: Hugsaðu hratt

3 SVÖR Í HVERJUM FLOKKI. SÁ VINNUR SEM FYLLIR FYRST ÚT LISTANN.

1	Staðir til að sækja örugg forrit			
2	Tæki sem hægt er að brjótast inn í			
3	Hlutir sem þú afritar			
4	Viðvörunarmerki í tölvupósti			
5	Merki þess að sími sé með spilliforrit			
6	Tegundir spilliforrita sem þú þekkir			
7	Skráartegundir sem ber að fara varlega með			
8	Leiðir sem spilliforrit kemst í tölvu			
9	Öruggar venjur sem þú getur byrjað á í dag			
10	Orð tengd netöryggi			
11	Hlutir til að gera eftir gagnaleka			
12	Ástæður fyrir því að uppfæra hugbúnað			
13	Dýr eða persónur með nöfn sem minna á spilliforrit			
14	Hlutir sem spilliforrit getur stolið			
15	Hlutir til að gera ef þú smelltir á rangan tengil			

Áfangi 8: Dæmisögur um netöryggi

Nýttu hugtökin sem þú hefur lært til að leysa raunveruleg dæmi hér að neðan.

DÆMISAGA 1: AFMÖRKUN LAUSNARHUGBÚNAÐAR Í FYRIRTÆKI



Aðstæður: Brotist hefur verið inn á staðarnet fyrirtækis með virku gíslatökuforriti. Lykilskráarnetþjónar eru farnir að sýna skráarendingar með .locked. Settu upp stefnur til að halda broti í skefjum.

Umræðuspurning: Lýstu skrefum til að hefta útbreiðslu og gerðu grein fyrir gagnaendurheimtarferlinu.

DÆMISAGA 2: MINNISINNSPRAUTUN SKRÁARLAUSS SPILLIFORRITS



Aðstæður: Greinandi greinir grunsamleg skriftumynstur sem keyra beint í rokgjörnu vinnsluminni kerfisins með venjulegum stjórnunartólum, en engar skaðlegar skrár eru á disknum.

Umræðuspurning: Útskýrðu minnisgreiningaraðferðina og tilgreindu verkfæri til að loka á skráalausa keyrslu.

Áfangi 9: Leystu dulmálið

Netöryggissérfræðingur ver netkerfiseignir gegn ógnaraðilum á netinu. Notaðu lykilinn „bókstafur í tölu“ hér að neðan til að afkóða skilaboðin með því að skrifa samsvarandi bókstafi í auðu reitina.

DULMÁLSLYKILL: STAFIR Í TÖLUR

A=1 Á=2 B=3 C=4 D=5 Đ=6 E=7 É=8 F=9 G=10 H=11 I=12

Í=13 J=14 K=15 L=16 M=17 N=18 O=19 Ó=20 P=21 Q=22 R=23 S=24

T=25 U=26 Ú=27 V=28 W=29 X=30 Y=31 Ý=32 Z=33 Þ=34 Æ=35 Ö=36

9	12	18	18	5	26		9	1	23	17	1		2
7	**18**	**5**	**1**	**21**	**26**	**18**	**15**	**25**	**26**	**17**		**17**	**7**	**6**
11	**7**	**10**	**6**	**26**	**18**	**1**	**23**	**28**	**36**	**15**	**25**	**26**	**18**

Afkóðuð skilaboð:

ÁBENDING: HVER TALA STENDUR FYRIR STÖÐU STAFSINS Í STAFRÓFINU (T.D. 1 = A, 2 = B, 36 = Ö).

Áfangi 10: Algengar spurningar um netöryggi – grunnstig (Hluti A)

Farðu yfir algengar spurningar og svör um varnir gegn netógnum.

Q1: Hvað er spilliforrit?

Skaðlegur hugbúnaður hannaður af ógnaraðilum til að skemma, taka yfir eða stela gögnum úr tækjum og netum.

Q2: Hver er munurinn á veiru og ormi?

Veira þarfnast aðgerðar manna (eins og að opna skrá) til að dreifast, en ormur dreifist sjálfkrafa um net.

Q3: Hvernig smitar Trójuhestur tölvu?

Það blekkir notendur með því að þykjast vera skaðlaust eða öruggt forrit og felur skaðlegan farm sinn inni í því.

Q4: Hvað er gíslatökuforrit (ransomware)?

Tegund spilliforrits sem dulkóðar skrár á skotmarkskerfinu og krefst fjárgreiðslu í skiptum fyrir afkóðunarlykilinn. [1]

Q5: Hvað er njósnaforrit (spyware)?

Skaðlegur hugbúnaður sem skráir leynilega lyklaborðsslög, lykilorð og vafravenjur notanda og sendir til árásaraðila.

Áfangi 10: Algengar spurningar um netöryggi – grunnstig (Hluti B)

Farðu yfir algengar spurningar og svör um varnir gegn netógnum.

Q6: Hvað þýðir sandkassakeyrsla (sandboxing)?

Að keyra grunsamlegar skrár í öruggu, einangruðu sýndarumhverfi til að fylgjast með hegðun þeirra án áhættu fyrir framleiðslukerfi.

Q7: Hvað er skráalaust spilliforrit (fileless malware)?

Spilliforrit sem keyrir beint í kerfisminni (RAM) með löglegum hjálparforritum og forðast að skrifa skrár á diskinn til að komast hjá einföldum skönnum.

Q8: Hvernig ver rótarsett (rootkit) spilliforrit?

Það felur skaðleg ferli og skrár, oft með því að grafa undan kjarna stýrikerfisins, svo veiruskannar geta misst af þeim.

Q9: Hvað er kvik atferlisvöktun?

Vírusvarnarskönnun sem fylgist með virkum ferlum í rauntíma til að loka á aðgerðir sem eru dæmigerðar fyrir spilliforrit, eins og fjöldadulkóðun skráa.

Q10: Hvers vegna er innilokun brýn við viðbrögð við atvikum?

Að einangra afhjúpaða endapunkta kemur í veg fyrir að virkur farmur spilliforrita dreifist til annarra tækja á netinu.

Áfangi 10: Algengar spurningar um öryggi – framhaldsstig (Hluti C)

Kannaðu ítarlega tæknilega þætti öryggisrammaverka, spilliforritagreiningar og gagnareglufylgni.

Q1: Hvernig komast höfundar spilliforrita framhjá vírusvörnum sem byggja á undirskriftum?

Þeir nota fjölbreytni (polymorphism), breyta kjötkássu og kóðabyggingu skrárinnar við hverja sýkingu en halda illgjörnu hegðuninni óbreyttri.

Q2: Hver er áhættan af tvínotatólum í spilliforritaherferðum?

Árásarmenn nota lögmæt stjórnunartól (eins og PowerShell eða Sysinternals) til að falla inn í venjulega netumferð, sem gerir uppgötvun erfiða.

Q3: Hvernig keyrir „process hollowing“ skaðlegan hleðslukóða?

Það ræsir lögmætt kerfisferli í biðstöðu, skiptir út kóða þess í minni fyrir spilliforrit og heldur áfram keyrslu.

Q4: Hvaða hlutverki gegnir stjórnþjónn (C2)?

Fjarnetþjónn í umsjón tölvuþrjóta sem sendir fyrirmæli og aukaforrit til spilliforrits sem keyrir á sýktum vélum.

Q5: Hvers vegna er erfitt að greina lyklaskráningu (keylogging)?

Einföld lyklaborðsnjósnaforrit nota lítið af örgjörvaauðlindum og fela ferli sín inni í lögmætum notendarýmistólum.

Áfangi 10: Algengar spurningar um öryggi – framhaldsstig (Hluti D)

Kannaðu ítarlega tæknilega þætti öryggisrammaverka, spilliforritagreiningar og gagnareglufylgni.

Q6: Hvernig tefur kóðadulbúningur greiningu á spilliforritum?

Það dulkóðar eða endurraðar frumkóðanum þannig að greiningartól og öryggisskannar geta ekki lesið hann.

Q7: Hvert er hlutverk ræsisýkils (bootkit)?

Rótarsett (rootkit) sem sýkir ræsiferlið (MBR, ræsigeira eða UEFI-fastbúnað) og keyrir því áður en stýrikerfið hleðst.

Q8: Hvernig greinir atferlisskönnun (heuristic) núlldagsógnir?

Það leitar að grunsamlegum kóðamynstrum og stjórnendaskipunum frekar en að leita að samsvarandi tætigildi í gagnagrunni.

Q9: Hver er ógnin af DLL-ráni (DLL hijacking)?

Að neyða lögmætt forrit til að hlaða skaðlegu kvikbundnu safni (DLL) með því að setja það í möppuslóð forritsins.

Q10: Hvernig nota sjálfvirkar greiningarlínur fyrir spilliforrit sýndarvæðingu?

Þeir keyra grunsamlegar skrár á mörgum sýndarvélum með mismunandi stýrikerfum og búa sjálfkrafa til hegðunarskrár og PCAP-skrár um netumferð.

Hluti 11: 10 staðreyndir um netöryggi og innsýn úr raunheimum

Farðu yfir raunverulegar staðreyndir um öryggisbrot, varnarkerfi og reglufylgnistaðla.

1. INNSÝN Í ÖRYGGI

Trójuhestar eru enn algeng leið til sýkingar því þeir fela skaðlegan kóða í forritum sem líta saklaus út.

2. INNSÝN Í ÖRYGGI

IC3 hjá FBI fékk yfir 3.600 kvartanir vegna kúgunarhugbúnaðar árið 2025 og tilkynnt tjón nam meira en 32 milljónum dala. [3]

3. INNSÝN Í ÖRYGGI

Ormar geta breiðst hratt út um net með því að nýta óuppfærða veikleika í samskiptareglum, eins og EternalBlue í SMB.

4. INNSÝN Í ÖRYGGI

Skráarlaust spilliforrit er erfitt að greina vegna þess að það keyrir í minni í gegnum lögmæt verkfæri og skilur fá ummerki eftir á diskinum.

5. INNSÝN Í ÖRYGGI

Greiningarsandkassar fara yfirleitt aftur í hreint skyndimynd eftir hverja keyrslu svo hvert próf hefjist í þekktu ástandi.

6. INNSÝN Í ÖRYGGI

Rótarsett (rootkits) geta breytt kerfiskalla kjarnans og skilað fölskum greiningarniðurstöðum til spilliforritaskanna.

7. ÖRYGGISINNSÝN

Kóðadulbúningur notar pökkunartól til að þjappa og fela raunverulega tvíundaruppbyggingu hleðslu spilliforrits.

8. ÖRYGGISINNSÝN

Fjölbreytilegt spilliforrit breytir kóða sínum, og þar með tætigildi skrárinnar, með hverju nýju afriti til að sneiða hjá undirskriftarathugunum.

9. ÖRYGGISINNSÝN

DLL-rán nýta sér leitarröð í stöðluðum stýrikerfum á borð við Windows.

10. INNSÝN Í ÖRYGGI

Öryggisfyrirtæki finna gríðarlegan fjölda nýrra spilliforritasýna daglega, svo undirskriftir þurfa stöðugar uppfærslur.

Tæknilegar heimildir og tilvísanir

Námsleiðbeiningarnar og gagnvirku þrautirnar eru unnar úr alþjóðlegum stöðlum NIST og OWASP og kröfum um persónuverndarsamræmi.

FRÆÐILEGAR HEIMILDIR OG HEIMILDIR ÚR ATVINNUGREININNI

[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

Lausnir: Áfangi 1 – Fjölval

1 Spurning 1 — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvað einkennir tróverja (Trojan horse)? → Það þykist vera lögmætur hugbúnaður til að blekkja notendur til að keyra það

2 Spurning 2 — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvaða gerð spilliforrits dulkóðar skrár og krefst greiðslu? → Kúgunarhugbúnaður

3 Spurning 3 — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvað táknar njósnahugbúnaður? → Spilliforrit sem er hannað til að fylgjast leynilega með lyklaborðsslögum og vafravirkni notenda

4 Spurning 4 — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvers vegna nota höfundar spilliforrita rótarsett (rootkits)? → Til að fela virk ferli og skaðlegar skrár fyrir stýrikerfinu

5 Spurning 5 — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvað merkir sandkassi (sandboxing) í greiningu spilliforrita? → Að keyra grunsamlegar skrár í einangruðu sýndarhólfi til að fylgjast örugglega með hegðun þeirra

Lausnir: Áfangi 2 – Satt eða ósatt

6 **Spurning 6** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Ósatt: ormar fjölga sér sjálfir og dreifast um net án nokkurra aðgerða notanda.

7 **Spurning 7** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Ósatt: auglýsingaforrit eru ekki alltaf meinlaus; mörg rekja vafur til að beina auglýsingum.

8 **Spurning 8** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Satt: hrein afrit án nettengingar endurheimta dulkóðaðar skrár án greiðslu, þótt stolin gögn geti enn lekið.

9 **Spurning 9** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Ósatt: undirskriftaskannar þurfa þekkt sýni og því geta ný núlldagsspilliforrit sloppið framhjá þeim.

10 **Spurning 10** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Skráarlaust spilliforrit keyrir skaðleg skriftur í kerfisminni og forðast að skrifa skrár á diskinn.

Orðalyklar og matskvarði

Einkunnaviðmið kennara: Gefðu 1 stig fyrir hverja rétta pörun (alls 8 stig) og hvert samhengishugtak (alls 6 stig).

ÁFANGI 4: LAUSNIR – PÖRUN HUGTAKA

D 1. TRÓJUHESTUR	F 2. GÍSLATÖKUFORRIT	A 3. NJÓSNAFORRIT	H 4. RÓTARSETT
G 5. SANDKASSI	C 6. AFMÖRKUN	E 7. WORM	B 8. SKRÁARLAUS

ÁFANGI 3: LAUSNIR – LYKILHUGTÖK

1 TRÓJUHESTUR	2 RANSOMWARE	3 NJÓSNAFORRIT	4 ROOTKIT
5 SANDKASSI	6 EINANGRUN		

ÁFANGI 6, VALKOSTUR: LAUSNIR – PÖRUN ORÐA

1 D – ROOTKIT	2 F – EINANGRUN	3 H – SKRÁARLAUST	4 G – ORMUR
5 B – RANSOMWARE	6 C – NJÓSNAFORRIT	7 A – TRÓJUHESTUR	8 E – SANDKASSI

UMRÆÐUATRIÐI FYRIR KENNARA

Lykilhugtök:
Athugaðu hvort nemendur geti útskýrt TRÓJUHESTUR, GÍSLATÖKUFORRIT og NJÓSNAFORRIT með eigin orðum og gefið dæmi um hvert hugtak.

Dæmisögur:
Biddu nemendur að styðja tillögur sínar með staðreyndum úr verkefnablaðinu en ekki ágiskunum.

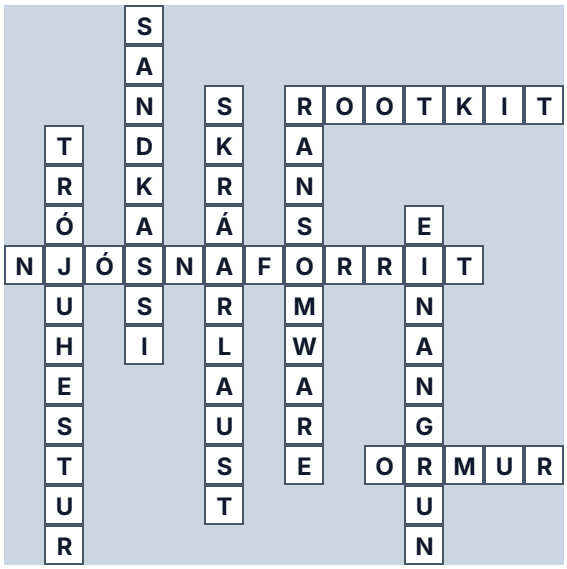
Mat á heimildum:
Biddu nemendur að sannreyna að minnsta kosti eina fullyrðingu í heimildum blaðsins og ræðið hvers vegna tölur, verð og reglur geta breyst með tímanum.

Lausnir við þrautum og athugasemdir fyrir kennara

LAUSN ORÐALEITAR

A	N	Đ	O	Đ	É	G	R	I	Đ	S	R	M	E	I
R	U	T	Ö	U	É	R	A	X	É	S	A	A	R	Ó
U	R	R	U	M	R	O	N	N	P	A	Ú	Þ	R	J
T	G	S	Ú	T	D	N	S	Æ	B	N	F	T	Ý	Y
S	N	Í	A	S	Ö	Æ	O	Æ	K	D	F	I	S	M
E	A	S	J	L	L	U	M	Ó	G	K	P	R	K	G
H	N	Ö	A	O	X	F	W	V	B	A	Æ	T	R	Æ
U	I	Á	G	L	Ö	G	A	J	O	S	P	N	Á	Ý
J	E	B	L	Ö	Æ	F	R	Þ	Ó	S	Y	V	A	K
Ó	V	P	Á	O	X	Ú	E	L	G	I	X	D	R	Þ
R	N	J	Ó	S	N	A	F	O	R	R	I	T	L	V
T	J	S	Á	Ý	Ö	Þ	M	T	R	Ý	I	Ó	A	Đ
A	D	R	O	O	T	K	I	T	J	R	Y	Ý	U	Ý
K	Í	H	Ú	H	F	Á	É	I	K	U	T	Y	S	S
Ö	E	H	É	T	D	A	L	P	B	Ö	M	J	T	X

LAUSN KROSSGÁTUNNAR



LEIÐBEININGAR FYRIR KENNARA UM LAUSNIR KROSSGÁTU

LÁRÉTT

3 lárétt: ROOTKIT Spilliforrit sem felur sig djúpt í kjarna kerfisins til að halda stjórnandavöldum (7 stafir)

6 lárétt: NJÓSNAFORRIT Forrit sem er hannað til að fylgjast leynilega með og skrá athafnir og innslátt notanda (12 stafir)

7 lárétt: ORMUR Sjálfafritandi spilliforrit sem dreifir sér um net án aðgerða manna (5 stafir)

LÓÐRÉTT

1 lóðrétt: SANDKASSI Einangrað sýndarumhverfi sem notað er til að greina skaðlegar skrár á öruggan hátt (9 stafir)

2 lóðrétt: SKRÁARLAUST Spilliforrit sem keyrir beint í vinnsluminni til að komast hjá greiningu diskaskanna (11 stafir)

3 lóðrétt: RANSOMWARE Spilliforrit sem dulkóðar geymslu kerfis og krefst greiðslu fyrir afhendingu lykils (10 stafir)

4 lóðrétt: TRÓJUHESTUR Skaðlegur hugbúnaður sem dulbýr sig sem meinlaust eða gagnlegt forrit (11 stafir)

5 lóðrétt: EINANGRUN Takmörkun á smituðum endapunktum til að koma í veg fyrir dreifingu skaðlegs farms (9 stafir)

Lausnir: Stafaruglingur og dulmál

Lausnalykill fyrir virkni um að raða orðaforða og Secret Cipher Challenge.

LYKILL ORÐARAÐAR

1. UEURHSTTÓRJ — TRÓJUHESTUR
2. TJNANRIÓORFS — NJÓSNAFORRIT
3. SAKASIDSN — SANDKASSI
4. MRUOR — ORMUR
5. AMEASWORRN — RANSOMWARE
6. IOKRTTO — ROOTKIT
7. GEUNRAINN — EINANGRUN
8. ULTRRSAKSAÁ — SKRÁARLAUST

LYKILL AÐ LEYNIDULMÁLSÞRAUT

"FINNDU FARMA Á ENDAPUNKTUM MEÐ HEGÐUNARVÖKTUN"

Lausnir dæmisagna

A Dæmisaga 1: Afmörkun lausnarhugbúnaðar í fyrirtæki

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Greining aðstæðna: Staðarnet fyrirtækis hefur verið brotist inn á með virkri gagnagíslatöku. Lykilskráaþjónar eru farnir að sýna skráarendingar með .locked. Komdu á stefnum um innilokun.
- Ráðlögð aðferð og lausn: Aftengdu alla netþjóna sem verða fyrir áhrifum frá staðarnetinu. Bindaðu enda á virkar stjórnendalotur. Endurheimtu óskemmdar skrár úr öruggu afritunarkerfi án nettengingar sem er skrifvarið.

B Dæmisaga 2: Minnisinnsprautun skráarlauss spilliforrits

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Greining aðstæðna: Greinandi finnur grunsamleg skriftumynstur sem keyra beint í rokgjörnu vinnsluminni kerfisins með hefðbundnum stjórnunartólum, en engar skaðlegar skrár eru á disknum.
- Ráðlögð aðferð og lausn: Einangraðu viðkomandi endapunkta og taktu fyrst minnismynd. Farðu yfir PowerShell- og WMI-skrár, lokaðu á óheimil skriftuforrit með AppLocker og endurræstu síðan til að hreinsa skaðlegan farm.