Ainm: _____ **Dáta:** _____ **Scór:** _____

Anailís ar bhogearraí mailíseacha agus maolú bagartha Treoir

Capaill Traí, ransomware, spiaireacht, rootkits, bosca gainimh fíorúlachta, coimeád

FORBHREATHNÚ FOGHLAMA AR ANAILÍS BHOGEARRAÍ MAILÍSEACHA

SLÁNAITHE
CRIPTIÚ SONRAÍ
Caighdeán AES 256-giotán

COMHLÍONTACH
CAIGHDEÁIN DHOMHANDA
Creataí GDPR agus CCPA

IONTAOBHAS NIALASACH
POLASAÍ ROCHTANA
Fíordheimhniú ilfhachtóra

Fáilte! Treoraíonn an paca gníomhaíochtaí seo thú trí anailís agus cosc bogearraí mailíseacha. Déanfaidh tú iniúchadh ar spiaire-bhogearraí, trójánaigh, ualaí lunnaíochta, uirlisí inbhéartinnealtóireachta, iompar rootkit, agus straitéisí coimeádta.

SEICPHOINTÍ NA BILEOGE OIBRE

- [ ] **Cuid 1-4: Máistrigh cibearshlándáil agus cosc bagairtí.**
- [ ] **Cuid 5-7: Réitigh tras-fhocail agus puzail cuardaigh focal.**
- [ ] **Cuid 8-9: Réitigh cás-staidéir agus dúshlán cód.**
- [ ] **Cuid 10: Déan athbhreithniú ar leathanaigh Ceisteanna Coitianta bunúsacha agus ardleibhéil.**
- [ ] **Cuid 11: Féach ar 10 bhfíric spéisiúla ón domhan fíor.**
- [ ] **Breis: dúshlán Smaoinigh go tapa.**

Oscail Treoir VPN.com ar Chibearshlándáil

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

Do threoirmhapa foghlama: maolú bogearraí mailíseacha

- Idirdhealaigh idir cineálacha bogearraí mailíseacha Trojan, péiste, agus rootkit.
- Forghníomhú bosca gainimh virtealaithe a chur i bhfeidhm le haghaidh anailís cóid.
- Dear pleananna srianta agus sláintíochta do phálasta ransomware gníomhacha.

TREOIRACHA AR ANAILÍS BHOGEARRAÍ MAILÍSEACHA

Freagair na ceisteanna ilrogha agus fíor/bréagach, comhlánaigh na habairtí le bearnaí leis an mbanc focal, meaitseáil sainmhínithe, agus réitigh an crosfhocal agus an cuardach focal. Cuir do chuid eolais i bhfeidhm ar mhaolú bogearraí mailíseacha. Críochnaigh leis an ngníomhaíocht bhreise Smaoinigh go tapa.

ANAILÍS AR BHOGEARRAÍ MAILÍSEACHA AGUS COINNEÁIL BAOIL FAOI SMACHT (RÉAMHRÁ)

Is bagairtí ardtionchair do chríochphointí agus d'fhreastalaithe iad cód mailíseach cosúil le Trojans, péisteanna agus ransomware. Déanann foirne slándála bogearraí mailíseacha a anailísiú laistigh de bhoscaí gainimh fíorúla agus cuireann siad rialuithe tapa leithlisithe líonra i bhfeidhm chun scaipeadh an lastais a chuimsiú.

LÉIGH GACH SEICPHOINTE GO CÚRAMACH AGUS ROGHNAIGH NÓ SCRÍOBH AN FREAGRA CEART.

Seicphointe 1: Dúshlán ilrogha

1 **1. Cad é saintréith chapall Traí?**

- A. Cuireann sé é féin i gcéill mar bhogearraí dlisteanacha chun úsáideoirí a mhealladh chun é a rith
- B. Atáirgeann sé é féin go huathoibríoch thar línte líonra áitiúil
- C. Ionfhabhtaíonn sé comhaid laistigh de bhoscaí gainimh fíorúla leithlisithe
- D. Idircheapann sé trácht soláthraí seirbhíse idirlín

2 **2. Cén cineál bogearraí mailíseacha a chriptíonn comhaid agus a éilíonn íocaíocht?**

- A. Ransomware
- B. Spiaunra
- C. Rootkit
- D. Adware

3 **3. Cad a léiríonn spiaireacht-bhogearraí?**

- A. Bogearraí mailíseacha atá deartha chun méarbhuillí agus gníomhaíochtaí brabhsálaí úsáideoirí a mhonatóiriú go rúnda
- B. Cód clár a fhorghníomhaítear taobh istigh de choimeádán fíorúil bosca gainimh
- C. Nuashonruithe frithbhogearraí mailíseacha arna n-íoslódáil ó chlárlanna bunachar sonraí
- D. Coigeartú uathoibríoch ar gheal scáileáin

4 **4. Cén fáth a n-úsáideann forbróirí bogearraí mailíseacha rootkits?**

- A. Próisis ghníomhacha agus comhaid mhailíseacha a cheilt ón gcóras oibriúcháin
- B. Luas próiseála LAP a mhéadú ar chríochphointí
- C. Chun comhaid bhunachair sonraí a chúltacú chuig cruinneacha slána scamall
- D. Saol bataire a fheabhsú ar ríomhairí glúine

5 **5. Cad is brí le bosca gainimh (sandboxing) in anailís bogearraí mailíseacha?**

- A. Comhaid amhrasacha a fhorghníomhú i gcromán fíorúil scoite chun iompar a bhreathnú go sábháilte
- B. Hashanna comhad a scanadh i gcoinne bunachar sonraí bagairtí aitheanta
- C. Cúltacaí bunachair sonraí a athchóiriú tar éis ionraidh
- D. Ródairí líonra áitiúil a dhícheangal ó línte poiblí

Seicphointe 2: Dúshlán Fíor nó Bréagach

6 Ceist 6

6. Éilíonn péisteanna ríomhaire idirghníomhú ó úsáideoir daonna chun iad féin a iomadú ar fud líonraí áitiúla.

Fíor Bréagach

7 Ceist 7

7. Bíonn bogearraí fógraíochta neamhdhochrach i gcónaí agus ní rianaíonn siad iompar úsáideora ná stair bhrabhsálaí.

Fíor Bréagach

8 Ceist 8

8. Ligeann athchóiriú cúltacaí glana as líne d'íospartaigh comhaid chriptithe a aisghabháil gan an t-airgead fuascailte a íoc.

Fíor Bréagach

9 Ceist 9

9. Stopann frithvíreas bunaithe ar shíniú bogearraí mailíseacha zero-day go hiontaofa sula bhfuil aon síniú ann dóibh.

Fíor Bréagach

10 Ceist 10

10. Rithtear bogearraí mailíseacha gan comhad scripteanna mailíseacha i gcuimhne an chórais, ag seachaint comhaid a scríobh ar an diosca.

Fíor Bréagach

Seicphointe 3: Príomhthéarmaí a chur isteach

Léigh gach abairt thíos agus líon isteach an bhearna leis an téarma ceart ón mBanc Focal.

1. Bogearraí mailíseacha faoi chlúdach clár áirgiúil sábháilte is ea _____ .

2. Is ionann _____ agus pálasta mailíseacha a ghlasálann córais bhunachair sonraí ar airgead.

3. Is ionann _____ agus loggálaithe eochracha a thaifeadann pasfhocail faoi rún.

4. Teastaíonn _____ chun folú go domhain laistigh d'eithne an chórais oibriúcháin.

5. Úsáidtear _____ fíorúil chun comhaid amhrasacha a anailísiú in áit scoite.

6. Teastaíonn _____ líonra láithreach chun scaipeadh pálasta bogearraí mailíseacha gníomhacha a stopadh.

BANC FOCAL FOCLÓIRE

BOSCA GAINIMH | GAN CHOMHAD | PÉIST | RANSOMWARE | ROOTKIT | SPIABHOGEARRAÍ | TEORANNÚ | TROIDEACH

Scríobh do fhreagraí anseo:

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

Seicphointe 4: Meaitseáil coincheapa slándála

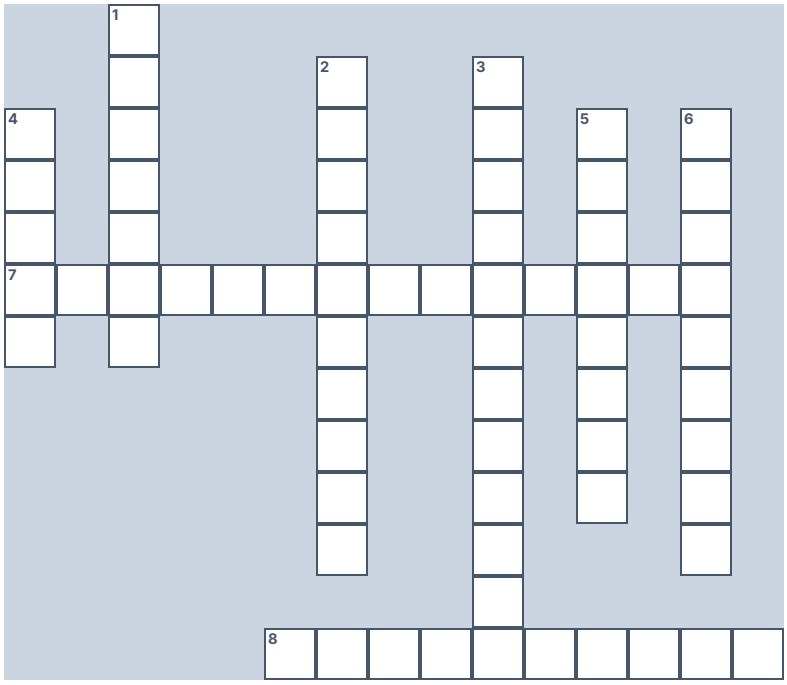
MEAITSEÁIL SAINMHÍNITHE

Meaitseáil gach téarma foclóra ar chlé lena shainmhíniú ceart ar dheis trí scríobh na litreach comhfhreagraí (A-H) sa bhosca ionchuir inlíonta.

	1. TRÓIÁNACH	A	Clár atá deartha chun gníomhaíocht agus ionchuir úsáideora a mhonatóiriú agus a thaifeadadh faoi rún.
	2. BOGEARRAÍ FUASCAILTE	B	Bogearraí mailíseacha a fhorghníomhaítear go díreach i RAM chun scanóirí diosca a sheachaint.
	3. BOGEARRAÍ SPIAIREACHTA	C	Críochphointí ionfhabhtaithe a shrianadh chun scaipeadh ualaí bagartha a chosc.
	4. ROOTKIT	D	Bogearraí mailíseacha faoi chaolchúis cláir fóntais neamhdhíobhálach nó úsáideach.
	5. BOSCA GAINIMH	E	Bogearraí mailíseacha féin-mhúnlaithe a scaipeann trasna líonraí gan gníomh daonna.
	6. COINNEÁIL	F	Bogearraí mailíseacha a chriptíonn stóras córais agus a éilíonn íocaíocht as eochair a sheachadadh.
	7. PÉIST	G	Timpeallacht fhíorúil leithlisithe a úsáidtear chun comhaid mhailíseacha a anailísiú go sábháilte.
	8. GAN COMHAD	H	Bogearraí mailíseacha Stealth a cheileann go domhain in eithne córais chun smacht riaracháin a choinneáil.

Seicphointe 5: Crosfhocal

Réitigh an crosfhocal trí litreacha a chlóscríobh sna boscaí bána gníomhacha. Freagraíonn na huimhreacha do na leideanna thíos.



TRASNA

7. Clár atá deartha chun gníomhaíocht agus ionchur úsáideora a mhonatóiriú agus a thaifeadadh faoi rún (14)

8. Bogearraí mailíseacha a fhorghníomhaítear go díreach i RAM chun brath ag scanóirí diosca a sheachaint (10)

SÍOS

1. Bogearraí mailíseacha folaithe a cheilíonn go domhain in eithne an chórais chun rialú riaracháin a choinneáil (7)

2. Bogearraí mailíseacha a chriptíonn stóras córais agus a éilíonn íocaíocht ar sheachadadh an eochair (10)

3. Timpeallacht fhíorúil scoite a úsáidtear chun comhaid mhailíseacha a anailísiú go sábháilte (12)

4. Bogearraí mailíseacha féin-mhacasamhlaithe a scaipeann thar líonraí gan gníomh daonna (5)

5. Críochphointí ionfhabhtaithe a theorannú chun scaipeadh pálasta bagartha a chosc (8)

6. Bogearraí mailíseacha atá faoi chlúdach clár áirgiúil neamhdhíobhálach nó úsáideach (9)

Seicphointe 5, rogha eile: Leideanna crosfhocail inrochtana

Is féidir le húsáideoirí léitheora scáileáin agus méarchláir freagraí na crosfhocal a chlóscríobh go díreach sna réimsí téacs thíos.

TRASNA

7 trasna: Clár atá deartha chun gníomhaíocht agus ionchur úsáideora a mhonatóiriú agus a thaifeadadh faoi rún (14 litir):

8 trasna: Bogearraí mailíseacha a fhorghníomhaítear go díreach i RAM chun brath ag scanóirí diosca a sheachaint (10 litir):

SÍOS

1 síos: Bogearraí mailíseacha folaithe a cheilíonn go domhain in eithne an chórais chun rialú riaracháin a choinneáil (7 litir):

2 síos: Bogearraí mailíseacha a chriptíonn stóras córais agus a éilíonn íocaíocht ar sheachadadh an eochair (10 litir):

3 síos: Timpeallacht fhíorúil scoite a úsáidtear chun comhaid mhailíseacha a anailísiú go sábháilte (12 litir):

4 síos: Bogearraí mailíseacha féin-mhacasamhlaithe a scaipeann thar líonraí gan gníomh daonna (5 litir):

5 síos: Críochphointí ionfhabhtaithe a theorannú chun scaipeadh pálasta bagartha a chosc (8 litir):

6 síos: Bogearraí mailíseacha atá faoi chlúdach clár áirgiúil neamhdhíobhálach nó úsáideach (9 litir):

Seicphointe 6: Cuardach focal i bhfolach

Aimsigh na 8 dtéarma eochair-fhoclóra atá i bhfolach san eangach thíos. Is féidir focail a bheith cothrománach, ingearach, nó trasnánach.

H Y J K V J Y R W Y P J I Z I
M J N A E I A A S A J F W E K
I Z K E K Q N N J A F O K N D
N N C D H I B S A P R L P W T
I I Y F Y S G O X W H F R T N
A U K R D T S M L P L M S H K
G P H Y P L W W U N Y Q Q B A
A L P M B H C A E D I O R T L
C I F I N Y B R Z Z Y B N V X
S M C F P W Q E Q T S I E P X
O S P I A B H O G E A R R A I
B H E T E O R A N N U Y C W L
F G G A N C H O M H A D H Z W
C O R J X X R K Z A N R Z R M
G S T I K T O O R W G L W J B

LIOSTA FOCAL FOCLÓIRE

TROIDEACH RANSOMWARE SPIABHOGEARRAI ROOTKIT BOSCAGAINIMH
TEORANNU PEIST GANCHOMHAD

Seicphointe 6, rogha eile: Meaitseáil foclóra inrochtana

Meaitseáil gach ceann de na 8 dtéarma foclóra ón Cuardach Focal lena sainmhíniú ceart trí scríobh na litreach (A-H) sa spás folamh.

TÉARMAÍ FOCLÓIRE

A. TROIDEACH

B. RANSOMWARE

C. SPIABHOGEARRAI

D. ROOTKIT

E. BOSCAGAINIMH

F. TEORANNU

G. PEIST

H. GANCHOMHAD

SAINMHÍNITHE AGUS GLEANNTA MEAITSEÁLA

1. Bogearraí mailíseacha folaithe a cheilíonn go domhain in eithne an chórais chun rialú riaracháin a choinneáil.

2. Críochphointí ionfhabhtaithe a theorannú chun scaipeadh pálasta bagartha a chosc.

3. Bogearraí mailíseacha a fhorghníomhaítear go díreach i RAM chun brath ag scanóirí diosca a sheachaint.

4. Bogearraí mailíseacha féin-mhacasamhlaithe a scaipeann thar líonraí gan gníomh daonna.

5. Bogearraí mailíseacha a chriptíonn stóras córais agus a éilíonn íocaíocht ar sheachadadh an eochair.

6. Clár atá deartha chun gníomhaíocht agus ionchur úsáideora a mhonatóiriú agus a thaifeadadh faoi rún.

7. Bogearraí mailíseacha atá faoi chlúdach clár áirgiúil neamhdhíobhálach nó úsáideach.

8. Timpeallacht fhíorúil scoite a úsáidtear chun comhaid mhailíseacha a anailísiú go sábháilte.

Seicphointe 7: Dúshlán focal measctha

Dí-mheascaigh na litreacha thíos chun príomhchoincheapa agus téarmaí cibearshlándála a nochtadh. Scríobh do chuid freagraí sna boscaí ionchuir a sholáthraítear.

1. EDIRTACHO
2. BPHIOASRGIAREA
3. BOIAMNSGHAIC
4. ITSPE
5. AMEASWORRN
6. IOKRTTO
7. TUANNERO
8. ACODGHAMHN

Gníomhaíocht bhreise: Smaoinigh go tapa

3 FHREAGRA DO GACH CATAGÓIR. BUAILEANN AN CHÉAD DUINE A LÍONANN AN LIOSTA.

1	Áiteanna chun aipeanna sábháilte a íoslódáil			
2	Feistí ar féidir hacáil a dhéanamh orthu			
3	Rudaí a dhéanann tú cúltaca díobh			
4	Comharthaí rabhaidh i ríomhphost			
5	Comharthaí go bhfuil bogearraí mailíseacha ar ghuthán			
6	Cineálacha bogearraí mailíseacha a bhfuil aithne agat orthu			
7	Cineálacha comhad ar cheart a bheith cúramach leo			
8	Bealaí a thagann bogearraí mailíseacha ar ríomhaire			
9	Nósanna sábháilte is féidir leat a thosú inniu			
10	Focail a bhaineann le cibearshlándáil			
11	Rudaí le déanamh tar éis sceitheadh sonraí			
12	Cúiseanna le bogearraí a nuashonrú			
13	Ainmhithe nó carachtair a bhfuil ainmneacha cosúil le bogearraí mailíseacha orthu			
14	Rudaí ar féidir le bogearraí mailíseacha iad a ghoid			
15	Rudaí le déanamh má chliceáil tú ar an nasc mícheart			

Seicphointe 8: Cás-staidéir ar chibearshlándáil

Cuir na coincheapa a d'fhoghlaim tú i bhfeidhm chun na cásanna fíorshaoil thíos a réiteach.

CÁS-STAIDÉAR 1: COINNEÁIL CHUID UALAIGH RANSOMWARE FIONTAIR

👷

Cás: Briseadh isteach ar líonra ceantair áitiúil corparáideach le ransomware gníomhach. Tá freastalaithe comhad tábhachtacha tosaithe ag taispeáint síntiúis comhad le .locked. Bunaigh polasaithe cuimsithe.

Ceist phlé: Déan mionchur síos ar na céimeanna coimeádta, agus déan achoimre ar an bprótacal aisghabhála sonraí.

CÁS-STAIDÉAR 2: INSTEALLADH CUIMHNE BOGEARRAÍ MAILÍSEACHA GAN COMHAD

👷

Cás: Braitheann anailísí patrúin scriptithe amhrasacha á rith go díreach i RAM luaineach an chórais ag baint úsáide as uirlisí caighdeánacha riaracháin, ach níl aon chomhaid mhailíseacha ar an diosca.

Ceist phlé: Mínigh an straitéis anailíse cuimhne, agus sonraigh uirlisí chun forghníomhú gan chomhad a bhlocáil.

Seicphointe 9: Díchódaigh an cód

Cosnaíonn gairmí cibearshlándála sócmhainní líonra ó aisteoirí bagartha ar líne. Úsáid an eochair Litir-go-Uimhir thíos chun an teachtaireacht a dhíchódú trí na litreacha comhfhreagracha a scríobh sna spásanna folmha.

EOCHAIR CHRIPTITHE LITIR-GO-UIMHIR

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

2	18	1	20	8		16	1	12	1	19	20	1		12	5

13	15	14	1	20	15	9	18	9

9	15	13	16	18	1	9	15	3	8	20	1

Teachtaireacht díchódaithe:

COMHAIRLE: FREAGRAÍONN GACH UIMHIR DO SHUÍOMH NA LITRE SIN SAN AIBÍTIR (M.SH. 1 = A, 2 = B, 26 = Z).

Seicphointe 10: Ceisteanna coitianta faoi chibearshlándáil – bunleibhéal (Cuid A)

Athbhreithnigh ceisteanna agus freagraí coitianta maidir le laghdú bagairtí ar líne.

Q1: Cad is bogearraí mailíseacha ann?

Bogearraí mailíseacha a dhearann gníomhaithe bagartha chun sonraí a lot, a fhuadach nó a ghoid ó ghléasanna agus ó líonraí.

Q2: Cad é an difríocht idir víreas agus péist?

Teastaíonn gníomh daonna (ar nós comhad a oscailt) ó víreas chun scaipeadh, agus scaipeann péist go huathoibríoch trasna líonraí.

Q3: Conas a ionfhabhtaíonn capall Traí ríomhaire?

Mealltar úsáideoirí leis trí ligean air gur clár neamhdhíobhálach nó sábháilte é, ag folú a luacha mhailíseach istigh.

Q4: Cad iad bogearraí fuascailte?

Cineál bogearraí mailíseacha a chriptíonn comhaid ar an gcóras sprice, ag éileamh íocaíochta airgeadais mar mhalairt ar an eochair dhíchriptithe. [1]

Q5: Cad iad bogearraí spiaireachta?

Bogearraí mailíseacha a thaifeadann i ndiamhair cnaipí a bhrúnn an t-úsáideoir, pasfhocail agus nósanna brabhsála chun iad a sheoladh chuig ionsaitheoirí.

Seicphointe 10: Ceisteanna coitianta faoi chibearshlándáil – bunleibhéal (Cuid B)

Athbhreithnigh ceisteanna agus freagraí coitianta maidir le laghdú bagairtí ar líne.

Q6: Cad is brí le bosca gainimh a úsáid?

Comhaid amhrasacha a rith i dtimpeallacht fhíorúil shlán, scoite chun a n-iompar a bhreathnú gan baol do chórais tháirgeachta.

Q7: Cad iad bogearraí mailíseacha gan chomhad?

Bogearraí mailíseacha a ritheann go díreach i gcuimhne an chórais (RAM) trí fhóntais dhlisteanacha, gan comhaid a scríobh ar an diosca chun scanóirí bunúsacha a sheachaint.

Q8: Conas a chosnaíonn rootkit bogearraí mailíseacha?

Folaíonn sé próisis agus comhaid mhailíseacha, go minic trí eithne an chórais oibriúcháin a fhoghail, mar sin féadfaidh scanóirí frithvíorais iad a chailleadh.

Q9: Cad é monatóireacht iompair dhinimiciúil?

Scanadh frithvíris a fhaireann próisis ghníomhacha i bhfíor-am chun gníomhartha is tipiciúil do bhogearraí mailíseacha a bhlocáil, amhail criptiú mórchomhad.

Q10: Cén fáth a bhfuil coimeád práinneach le linn freagra eachtra?

Cuireann leithlisiú críochphointí comhréitithe cosc ar phaicéid bhogearraí mailíseacha ghníomhacha leathadh chuig gléasanna líonra eile.

Seicphointe 10: Ceisteanna coitianta faoi shlándáil – ardleibhéal (Cuid C)

Déan iniúchadh ar ghnéithe teicniúla ardleibhéil de chreataí slándála, anailís bogearraí mailíseacha, agus comhlíonadh sonraí.

Q1: Conas a sheachnaíonn forbróirí bogearraí mailíseacha scanóirí frithvíorais bunaithe ar shínithe?

Úsáideann siad polaimorfacht, ag athrú hash agus struchtúr cód an chomhaid le gach ionfhabhtú agus an t-iompar mailíseach céanna á choinneáil.

Q2: Cad é riosca uirlisí dé-úsáide in fheachtais bhogearraí mailíseacha?

Úsáideann ionsaitheoirí uirlisí riaracháin dleathacha (amhail PowerShell nó Sysinternals) chun meascadh isteach le gnáthtrácht líonra, rud a fhágann go bhfuil sé deacair iad a bhrath.

Q3: Conas a fheidhmíonn process hollowing ualaí mailíseacha?

Seolann sé próiseas córais dlisteanach i stát ar fionraí, cuireann sé cód cuimhne ina áit le bogearraí mailíseacha, agus atosaíonn sé forghníomhú.

Q4: Cad é ról freastalaí Ordaithe agus Rialaithe (C2)?

Freastalaí iargúlta arna oibriú ag hackeálaithe chun treoracha agus pálastaí a sheoladh chuig bogearraí mailíseacha atá ag rith ar mheaisíní a chuaigh i gcontúirt.

Q5: Cén fáth a bhfuil sé deacair logáil eochracha a bhrath?

Úsáideann keyloggers bunúsacha íosmhéid acmhainní LAP agus ceileann siad a bpróisis laistigh d'fhóntais dhleathacha spáis úsáideora.

Seicphointe 10: Ceisteanna coitianta faoi shlándáil – ardleibhéal (Cuid D)

Déan iniúchadh ar ghnéithe teicniúla ardleibhéil de chreataí slándála, anailís bogearraí mailíseacha, agus comhlíonadh sonraí.

Q6: Conas a mhoillíonn doiléiriú cóid anailís ar bhogearraí mailíseacha?

Criptíonn nó athordaíonn sé an cód foinse, rud a fhágann nach féidir le huirlisí anailísí agus scanóirí slándála é a léamh.

Q7: Cad é feidhm bootkit?

Rootkit a ionfhabhtaíonn an próiseas tosaithe (an MBR, an teascán tosaithe nó firmware UEFI), ionas go ritheann sé sula luchtaítear an córas oibriúcháin.

Q8: Conas a aithníonn scanadh heoragnóiseach bagairtí zero-day?

Scanann sé patrúin chóid amhrasacha agus orduithe riaracháin seachas hais atá ag teacht le bunachar sonraí a lorg.

Q9: Cad é an bhagairt a bhaineann le fuadach DLL?

Iallach a chur ar aip dhlisteanach leabharlann nasctha dhinimiciúil (DLL) mhailíseach a luchtú trí í a chur i gcosán eolaire na haipe.

Q10: Conas a úsáideann píblínte uathoibrithe anailíse bogearraí mailíseacha fíorúlú?

Ritheann siad comhaid amhrasacha thar il-VManna OS, ag giniúint logaí iompair agus comhaid PCAP líonra go huathoibríoch.

Cuid 11: 10 bhFíric agus Léargas Cibearshlándála ón Domhan Fíor

Athbhreithnigh fíricí fíordhomhanda maidir le sáruithe slándála, sásraí cosanta, agus caighdeáin chomhlíonta.

1. EOLAS SLÁNDÁLA

Is modh ionfhabhtaithe coitianta iad capaill Traí i gcónaí, mar go bhfolaíonn siad cód mailíseach laistigh de chláir a bhfuil cuma neamhdhíobhálach orthu.

2. EOLAS SLÁNDÁLA

Fuair IC3 an FBI breis agus 3,600 gearán ransomware in 2025, agus sáraíonn na caillteanais tuairiscithe $32 milliún. [3]

3. EOLAS SLÁNDÁLA

Is féidir le péisteanna scaipeadh go tapa trasna líonraí trí leochaileachtaí prótacail gan paiste a shaothrú, amhail EternalBlue in SMB.

4. EOLAS SLÁNDÁLA

Tá bogearraí mailíseacha gan comhad deacair a bhrath toisc go ritheann siad i gcuimhne trí uirlisí dleathacha agus gur beag rian a fhágann siad ar an diosca.

5. EOLAS SLÁNDÁLA

De ghnáth filleann boscaí gainimh anailíse ar bhrúdhonn glan tar éis gach rite ionas go dtosaíonn gach tástáil ó staid aitheanta.

6. EOLAS SLÁNDÁLA

Is féidir le rootkits glaonna córais eithne a mhodhnú, ag tuairisciú torthaí diagnóiseacha bréagacha do scanóirí frithbhogearraí mailíseacha.

7. EOLAS SLÁNDÁLA

Úsáideann obfuscation cód uirlisí pacála chun struchtúr fíor chuid ualaigh dhénártha bogearraí mailíseacha a chomhbhrú agus a cheilt.

8. EOLAS SLÁNDÁLA

Athraíonn bogearraí mailíseacha polaimorfacha a gcód, agus mar sin hash a gcomhaid, le gach cóip nua chun seiceálacha sínithe a sheachaint.

9. EOLAS SLÁNDÁLA

Úsáideann fuadach DLL cumraíochtaí ord cuardaigh i ngnáthchórais oibriúcháin ar nós Windows.

10. EOLAS SLÁNDÁLA

Aimsíonn díoltóirí slándála líon ollmhór samplaí nua bogearraí mailíseacha gach lá, mar sin ní mór sínithe a nuashonrú go seasta.

Tagairtí teicniúla agus foinsí

Tá an treoirleabhar staidéir agus na mearaithe idirghníomhacha curtha le chéile ó chaighdeáin dhomhanda NIST, OWASP agus chomhlíonta príobháideachta sonraí.

TAGAIRTÍ ACADÚLA AGUS TIONSCAIL

[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

Freagraí: Seicphointe 1 – Ilrogha

1 **Ceist 1** — **Freagra ceart: A**

NÓTA DON MHÚINTEOIR

Cad é saintréith chapall Traí? → Cuireann sé é féin i gcéill mar bhogearraí dlisteanacha chun úsáideoirí a mhealladh chun é a rith

2 **Ceist 2** — **Freagra ceart: A**

NÓTA DON MHÚINTEOIR

Cén cineál bogearraí mailíseacha a chriptíonn comhaid agus a éilíonn íocaíocht? → Ransomware

3 **Ceist 3** — **Freagra ceart: A**

NÓTA DON MHÚINTEOIR

Cad a léiríonn spiaireacht-bhogearraí? → Bogearraí mailíseacha atá deartha chun méarbhuillí agus gníomhaíochtaí brabhsálaí úsáideoirí a mhonatóiriú go rúnda

4 **Ceist 4** — **Freagra ceart: A**

NÓTA DON MHÚINTEOIR

Cén fáth a n-úsáideann forbróirí bogearraí mailíseacha rootkits? → Próisis ghníomhacha agus comhaid mhailíseacha a cheilt ón gcóras oibriúcháin

5 **Ceist 5** — **Freagra ceart: A**

NÓTA DON MHÚINTEOIR

Cad is brí le bosca gainimh (sandboxing) in anailís bogearraí mailíseacha? → Comhaid amhrasacha a fhorghníomhú i gcromán fíorúil scoite chun iompar a bhreathnú go sábháilte

Freagraí: Seicphointe 2 – Fíor nó Bréagach

6 **Ceist 6** — **Freagra ceart: Bréagach**

NÓTA DON MHÚINTEOIR

Bréagach: déanann péisteanna iad féin a mhacasamhlú agus scaipeann siad trasna líonraí gan aon ghníomh úsáideora.

7 **Ceist 7** — **Freagra ceart: Bréagach**

NÓTA DON MHÚINTEOIR

Bréagach: ní bhíonn adware gan dochar i gcónaí; rianaíonn cuid mhór de brabhsáil chun fógraí a spriocdhíriú.

8 **Ceist 8** — **Freagra ceart: Fíor**

NÓTA DON MHÚINTEOIR

Fíor: athchóiríonn cúltacaí glana as líne comhaid chriptithe gan íoc, cé go bhféadfadh sonraí goidte sceitheadh fós.

9 **Ceist 9** — **Freagra ceart: Bréagach**

NÓTA DON MHÚINTEOIR

Bréagach: teastaíonn sampla aitheanta ó scanóirí sínithe, mar sin is féidir le bogearraí mailíseacha zero-day nua-nua dul thar bráid.

10 **Ceist 10** — **Freagra ceart: Fíor**

NÓTA DON MHÚINTEOIR

Rithtear bogearraí mailíseacha gan comhad scripteanna mailíseacha i gcuimhne an chórais, ag seachaint comhaid a scríobh ar an diosca.

Eochracha foclóra agus rúibric mharcála

Rúbraic ghrádaithe don mhúinteoir: Bronn 1 phointe do gach meaitseáil cheart (8 pointe san iomlán) agus téarma comhthéacs (6 pointe san iomlán).

SEICPHOINTE 4: FREAGRAÍ – MEAITSEÁIL COINCHEAPA

D 1. TRÓIÁNACH	F 2. BOGEARRAÍ FUASCAILTE	A 3. BOGEARRAÍ SPIAIREACHTA	H 4. ROOTKIT
G 5. BOSCA GAINIMH	C 6. COINNEÁIL	E 7. PÉIST	B 8. GAN COMHAD

SEICPHOINTE 3: FREAGRAÍ – PRÍOMHTHÉARMAÍ

1 TROIDEACH	2 RANSOMWARE	3 SPIABHOGEARRAÍ	4 ROOTKIT
5 BOSCA GAINIMH	6 TEORANNÚ		

SEICPHOINTE 6, ROGHA EILE: FREAGRAÍ – MEAITSEÁIL FOCAL

1 D – ROOTKIT	2 F – TEORANNU	3 H – GANCHOMHAD	4 G – PEIST
5 B – RANSOMWARE	6 C – SPIABHOGEARRAI	7 A – TROIDEACH	8 E – BOSCAGAINIMH

NÓTAÍ PLÉ DO MHÚINTEOIRÍ

Príomhthéarmaí:
Seiceáil an féidir leis na daltaí TRÓIÁNACH, BOGEARRAÍ FUASCAILTE agus BOGEARRAÍ SPIAIREACHTA a mhíniú ina bhfocail féin agus sampla a thabhairt de gach ceann.

Cás-staidéir:
Iarr ar na daltaí a moltaí a bhunú ar fhíricí ón mbileog oibre, ní ar thuairimí.

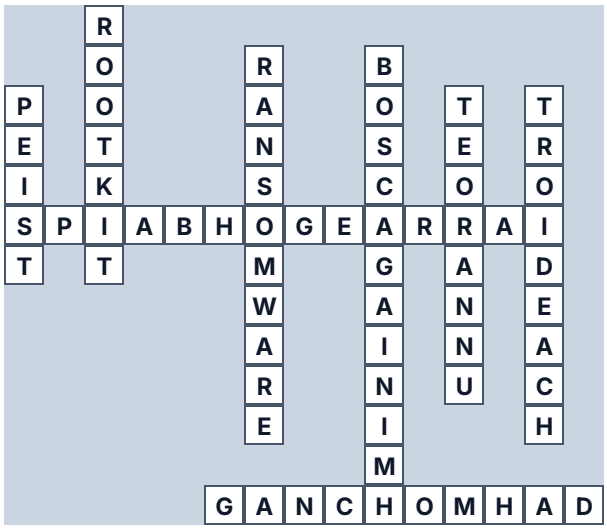
Measúnú foinsí:
Iarr ar na daltaí ráiteas amháin ar a laghad a fhíorú i bhfoinsí na bileoige agus pléigí cén fáth a bhféadfadh figiúirí, praghsanna agus rialacha athrú le himeacht ama.

Eochracha Puzal agus Nótaí don Mhúinteoir

CUR CHUN CINN FOCLÓIR CUARDAIGH

H	Y	J	K	V	J	Y	R	W	Y	P	J	I	Z	I
M	J	N	A	E	I	A	A	S	A	J	F	W	E	K
I	Z	K	E	K	Q	N	N	J	A	F	O	K	N	D
N	N	C	D	H	I	B	S	A	P	R	L	P	W	T
I	I	Y	F	Y	S	G	O	X	W	H	F	R	T	N
A	U	K	R	D	T	S	M	L	P	L	M	S	H	K
G	P	H	Y	P	L	W	W	U	N	Y	Q	Q	B	A
A	L	P	M	B	H	C	A	E	D	I	O	R	T	L
C	I	F	I	N	Y	B	R	Z	Z	Y	B	N	V	X
S	M	C	F	P	W	Q	E	Q	T	S	I	E	P	X
O	S	P	I	A	B	H	O	G	E	A	R	R	A	I
B	H	E	T	E	O	R	A	N	N	U	Y	C	W	L
F	G	G	A	N	C	H	O	M	H	A	D	H	Z	W
C	O	R	J	X	X	R	K	Z	A	N	R	Z	R	M
G	S	T	I	K	T	O	O	R	W	G	L	W	J	B

TUAIRISC CROSSWORD



TREOIR DON MHÚINTEOIR AR FHREAGRAÍ CROSFHOCAIL

TRASNA

7 trasna: SPIABHOGEARRAI Clár atá deartha chun gníomhaíocht agus ionchur úsáideora a mhonatóiriú agus a thaifeadadh faoi rún (14 litir)

8 trasna: GANCHOMHAD Bogearraí mailíseacha a fhorghníomhaítear go díreach i RAM chun brath ag scanóirí diosca a sheachaint (10 litir)

SÍOS

1 síos: ROOTKIT Bogearraí mailíseacha folaithe a cheilíonn go domhain in eithne an chórais chun rialú riaracháin a choinneáil (7 litir)

2 síos: RANSOMWARE Bogearraí mailíseacha a chriptíonn stóras córais agus a éilíonn íocaíocht ar sheachadadh an eochair (10 litir)

3 síos: BOSCAGAINIMH Timpeallacht fhíorúil scoite a úsáidtear chun comhaid mhailíseacha a anailísiú go sábháilte (12 litir)

4 síos: PEIST Bogearraí mailíseacha féin-mhacasamhlaithe a scaipeann thar líonraí gan gníomh daonna (5 litir)

5 síos: TEORANNU Críochphointí ionfhabhtaithe a theorannú chun scaipeadh pálasta bagartha a chosc (8 litir)

6 síos: TROIDEACH Bogearraí mailíseacha atá faoi chlúdach clár áirgiúil neamhdhíobhálach nó úsáideach (9 litir)

Eochair na bhfocal measctha agus réiteach an chóid

Eochair ghrádaithe don ghníomhaíocht dhíchuachta foclóra agus don Dúshlán Cód Rúnda.

EOCHAIR NA bhFOCAL DÍSCRAMBLAITHE

1.	EDIRTACHO	TROIDEACH	5.	AMEASWORRN	RANSOMWARE
2.	BPHIOASRGIAREA	SPIABHOGEARRAI	6.	IOKRTTO	ROOTKIT
3.	BOIAMNSGHAIC	BOSCAGAINIMH	7.	TUANNERO	TEORANNU
4.	ITSPE	PEIST	8.	ACODGHAMHN	GANCHOMHAD

EOCHAIR DHÚSHLÁN AN CHÓID RÚNDA

"BRATH PALASTA LE MONATOIRI IOMPRAIOCHTA"

Freagraí na gcás-staidéar

A Cás-staidéar 1: Coinneáil chuid ualaigh Ransomware fiontair

Réiteach don mhúinteoir

TREOIRLÍNE GRÁDÚ

Ba cheart do fhreagraí na mac léinn na pointí seo a leanas a chlúdach:

- Anailís cháis: Tá líonra ceantair áitiúil corparáideach sáraithe ag ransomware gníomhach. Tá síntí comhaid .locked ag taispeáint ar phríomhfhreastalaithe comhad. Bunaigh polasaithe coinneála.
- Straitéis mholta agus réiteach: Dícheangail gach freastalaí atá buailte den líonra ceantair áitiúil. Cuir deireadh le seisiúin riaracháin ghníomhacha. Athchóirigh comhaid nár compromisíodh ó chóras cúltaca as líne slán, cosanta ar scríobh.

B Cás-staidéar 2: Instealladh cuimhne bogearraí mailíseacha gan comhad

Réiteach don mhúinteoir

TREOIRLÍNE GRÁDÚ

Ba cheart do fhreagraí na mac léinn na pointí seo a leanas a chlúdach:

- Anailís cháis: Braitheann anailísí patrúin scripte amhrasacha ag rith go díreach i RAM éagonrach an chórais ag úsáid uirlisí riaracháin chaighdeánacha, ach níl aon chomhaid mhailíseacha ar an diosca.
- Straitéis agus réiteach molta: Scoilt na críochphointí atá buailte agus gabh íomhá chuimhne ar dtús. Athbhreithnigh logaí PowerShell agus WMI, bloc scripteanna neamhcheadaithe le AppLocker, ansin atosaigh chun an t-ualach a ghlanadh.