Nimi: _____ Päivämäärä: _____ Pisteet: _____

Haittaohjelma-analyysi ja uhkien hallinta Opas

Troijalaiset, kiristyshaittaohjelmat, vakoiluohjelmat, rootkitit, virtualisoinnin hiekkalaatikot, eristäminen

HAITTAOHJELMA-ANALYYSIN OPPIMISKATSAUS

SUOJATTU
TIETOJEN SALAUS
256-bittinen AES-standardi

LAINMUKAINEN
GLOBAALIT STANDARDIT
GDPR- ja CCPA-säädökset

NOLLALUOTTAMUS
KÄYTTÖKÄYTÄNTÖ
Monivaiheinen tunnistautuminen

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: haittaohjelmien analyysi ja ehkäisy. Tutustut vakoiluohjelmiin, troijalaisiin, kiristysohjelmien haittakuormiin, takaisinmallinnustyökaluihin, rootkit-ohjelmien toimintaan ja eristysstrategioihin.

TEHTÄVÄMONISTEEN TARKISTUSPISTEET

- [ ] **Osat 1–4: Hallitse kyberturvallisuus ja uhkien ehkäisy.**
- [ ] **Osat 5–7: Ratkaise ristisanatehtäviä ja sanahakuja.**
- [ ] **Osat 8–9: Ratkaise tapaustutkimuksia ja salakirjoitushaaste.**
- [ ] **Osa 10: Tarkista perus- ja jatkotason UKK-sivut.**
- [ ] **Osa 11: Tutustu 10 mielenkiintoiseen tosielämän faktaan.**
- [ ] **Bonus: Nopeat vastaukset -haaste.**

Avaa VPN.comin kyberturvallisuusopas

URL: https://www.vpn.com/fi/kyberturvallisuus/haittaohjelma/

Oppimispolkusi: haittaohjelmien torjunta

- Erota toisistaan troijalaiset, madot ja rootkitit haittaohjelmatyyppeinä.
- Toteuta hiekkalaatikkovirtualisoitu suoritus koodin analysointia varten.
- Suunnittele eristys- ja puhdistussuunnitelmia aktiivisille kiristysohjelmien hyötykuormille.

HAITTAOHJELMA-ANALYYSIN OPAS: OHJEET

Vastaa monivalinta- ja tosi/epätosi-kysymyksiin, täydennä aukkolauseet sanapankin avulla, yhdistä määritelmät sekä ratkaise ristisanatehtävä ja sanahaku. Sovella osaamistasi näihin aiheisiin: haittaohjelmien torjunta. Lopuksi bonustehtävä Nopeat vastaukset.

HAITTAOHJELMA-ANALYYSI JA UHKIEN HALLINTA (JOHDANTO)

Haitallinen koodi, kuten troijalaiset, madot ja kiristyshaittaohjelmat, aiheuttaa suuria uhkia päätelaitteille ja palvelimille. Tietoturvatiimit analysoivat haittaohjelmia virtuaalisissa hiekkalaatikoissa ja eristävät verkon nopeasti estääkseen haitallisen sisällön leviämisen.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1 **1. Mikä on troijalaisen määrittävä ominaisuus?**

- A. Se esiintyy aitona ohjelmistona huijatakseen käyttäjiä suorittamaan sen
- B. Se monistuu automaattisesti paikallisverkon linjoilla
- C. Se tartuttaa tiedostoja eristetyissä virtuaalisissa hiekkalaatikoissa
- D. Se sieppaa internetpalveluntarjoajan liikenteen

2 **2. Minkä tyyppinen haittaohjelma salaa tiedostot ja vaatii maksua?**

- A. Kiristyshaittaohjelma
- B. Vakoiluohjelma
- C. Rootkit
- D. Mainosohjelma

3 **3. Mikä edustaa vakoiluohjelmaa?**

- A. Haittaohjelma, joka on suunniteltu seuraamaan salaa käyttäjän näppäilyjä ja selaintoimintaa
- B. Ohjelmakoodi, joka suoritetaan hiekkalaatikoidussa virtuaalikontissa
- C. Haittaohjelmientorjuntapäivitykset, jotka ladataan tietokantarekistereistä
- D. Näytön kirkkauden automaattinen säätö

4 **4. Miksi haittaohjelmakehittäjät käyttävät rootkit-ohjelmia?**

- A. Piilottaa aktiiviset prosessit ja haitalliset tiedostot käyttöjärjestelmältä
- B. Nopeuttaa suorittimen käsittelynopeutta päätelaitteissa
- C. Tietokantatiedostojen varmuuskopiointi turvallisiin pilviholveihin
- D. Kannettavien akunkeston parantamiseksi

5 **5. Mitä hiekkalaatikkoeristys (sandboxing) tarkoittaa haittaohjelma-analyysissa?**

- A. Epäilyttävien tiedostojen suorittaminen eristetyssä virtuaalisessa holvissa käyttäytymisen turvalliseksi tarkkailemiseksi
- B. Tiedostotiivisteiden vertailu tunnettujen uhkien tietokantoihin
- C. Tietokantavarmuuskopioiden palauttaminen tunkeutumisen jälkeen
- D. Paikallisten verkkoreitittimien irrottaminen julkisista linjoista

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Tietokonemadot vaativat ihmiskäyttäjän toimintaa levitäkseen paikallisverkoissa.

- ◯ Tosi
- ◯ Epätosi

7 Kysymys 7

7. Mainosohjelmat ovat aina vaarattomia eivätkä seuraa käyttäjän toimintaa tai selainhistoriaa.

- ◯ Tosi
- ◯ Epätosi

8 Kysymys 8

8. Puhtaiden offline-varmuuskopioiden palauttaminen antaa uhrien palauttaa salatut tiedostot maksamatta lunnaita.

- ◯ Tosi
- ◯ Epätosi

9 Kysymys 9

9. Allekirjoituspohjainen virustorjunta pysäyttää luotettavasti nollapäivähaittaohjelmat ennen kuin niille on olemassa allekirjoitusta.

- ◯ Tosi
- ◯ Epätosi

10 Kysymys 10

10. Tiedostoton haittaohjelma suorittaa haitallisia skriptejä järjestelmämuistissa välttäen tiedostojen kirjoittamista levylle.

- ◯ Tosi
- ◯ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

Lue jokainen alla oleva lause ja täytä aukko oikealla termillä sanapankista.

1. Turvalliseksi apuohjelmaksi naamioitu haittaohjelma on _____ .

2. Tietokantajärjestelmät rahaa vastaan lukitsevat haitalliset hyötykuormat ovat tyyppiä _____ .

3. Salasanoja salaa tallentavat näppäinloggaajat ovat tyyppiä _____ .

4. Käyttöjärjestelmän ytimeen syvälle piiloutuva haittaohjelmatyyppi on _____ .

5. Epäilyttävien tiedostojen analysointiin eristetyssä holvissa tarvitaan virtuaalinen _____ .

6. Aktiivisten haittaohjelmien leviämisen pysäyttämiseksi tarvitaan verkon välitön _____ .

SANASTON SANAPANKKI

ERISTÄMINEN HIEKKALAATIKKO LUNNASOHJELMA MATO ROOTKIT TIEDOSTOTON TROIJALAINEN VAKOILUOHJELMA

Kirjoita vastauksesi tähän:

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

Tarkistuspiste 4: Tietoturvakäsitteiden yhdistäminen

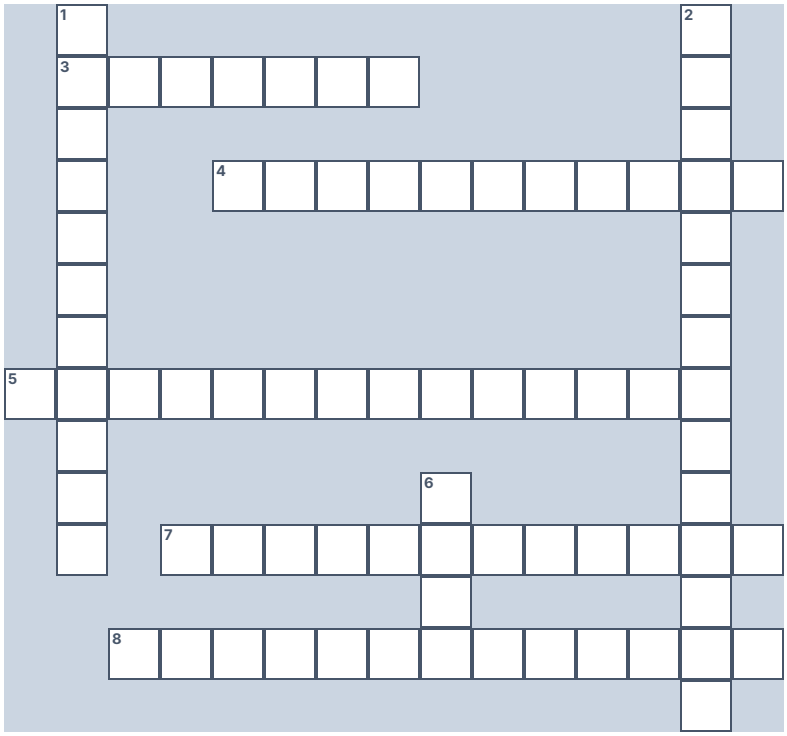
MÄÄRITELMIEN YHDISTÄMINEN

Yhdistä kukin vasemman puolen sanastotermi oikean puolen oikeaan määritelmään kirjoittamalla vastaava kirjain (A–H) täytettävään kenttään.

☐	1. TROJALAINEN	A	Ohjelma, joka on suunniteltu seuraamaan ja tallentamaan käyttäjän toimintaa ja syötteitä salaa.
☐	2. KIRISTYSHAITTAOHJELMA	B	Haittaohjelma, joka suoritetaan suoraan RAM-muistissa levytarkistimien havaitsemisen välttämiseksi.
☐	3. VAKOILUOHJELMA	C	Tartunnan saaneiden päätelaitteiden rajoittaminen uhkakuormien leviämisen estämiseksi.
☐	4. ROOTKIT	D	Haitallinen ohjelmisto, joka on naamioitu vaarattomaksi tai hyödylliseksi apuohjelmaksi.
☐	5. HIEKKALAATIKKO	E	Itseään kopioiva haittaohjelma, joka leviää verkoissa ilman ihmisen toimia.
☐	6. ERISTÄMINEN	F	Haittaohjelma, joka salaa järjestelmän tallennustilan ja vaatii maksua avaimen luovutuksesta.
☐	7. MATO	G	Eristetty virtuaaliympäristö, jota käytetään haitallisten tiedostojen turvalliseen analysointiin.
☐	8. TIEDOSTOTON	H	Piiloutuva haittaohjelma, joka kätkeytyy syvälle järjestelmän ytimiin säilyttääkseen ylläpitäjän hallinnan.

Tarkistuspiste 5: Ristikko

Ratkaise ristikko kirjoittamalla kirjaimia aktiivisiin valkoisiin ruutuihin. Numerot vastaavat alla olevia vihjeitä.



VAAKASUORAAN

3. Piilottelun hallitseva haittaohjelma, joka piiloutuu syvälle järjestelmän ytimeen säilyttääkseen ylläpitäjän hallinnan. (7)

4. Haittaohjelma, joka suoritetaan suoraan RAM-muistissa levyskannereiden havaitsemisen välttämiseksi. (11)

5. Eristetty virtuaaliympäristö, jossa haitallisia tiedostoja analysoidaan turvallisesti. (14)

7. Haitallinen ohjelma, joka on naamioitu harmittomaksi tai hyödylliseksi apuohjelmaksi. (12)

8. Haittaohjelma, joka salaa järjestelmän tallennustilan ja vaatii maksua avaimen toimittamisesta. (13)

PYSTYSUORAAN

1. Tartunnan saaneiden päätepisteiden rajoittaminen uhkien hyötykuormien leviämisen estämiseksi. (11)

2. Ohjelma, joka on suunniteltu salaa seuraamaan ja tallentamaan käyttäjän toimia ja syötteitä. (14)

6. Itseään kopioiva haittaohjelma, joka leviää verkoissa ilman ihmisen toimia. (4)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

Näytönlukijan ja näppäimistön käyttäjät voivat kirjoittaa ristikon vastaukset suoraan alla oleviin tekstikenttiin.

VAAKASUORAAN

3 vaakasuoraan: Piilottelun hallitseva haittaohjelma, joka piiloutuu syvälle järjestelmän ytimeen säilyttääkseen ylläpitäjän hallinnan. (7 kirjainta):

4 vaakasuoraan: Haittaohjelma, joka suoritetaan suoraan RAM-muistissa levyskannereiden havaitsemisen välttämiseksi. (11 kirjainta):

5 vaakasuoraan: Eristetty virtuaaliympäristö, jossa haitallisia tiedostoja analysoidaan turvallisesti. (14 kirjainta):

7 vaakasuoraan: Haitallinen ohjelma, joka on naamioitu harmittomaksi tai hyödylliseksi apuohjelmaksi. (12 kirjainta):

8 vaakasuoraan: Haittaohjelma, joka salaa järjestelmän tallennustilan ja vaatii maksua avaimen toimittamisesta. (13 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Tartunnan saaneiden päätepisteiden rajoittaminen uhkien hyötykuormien leviämisen estämiseksi. (11 kirjainta):

2 pystysuoraan: Ohjelma, joka on suunniteltu salaa seuraamaan ja tallentamaan käyttäjän toimia ja syötteitä. (14 kirjainta):

6 pystysuoraan: Itseään kopioiva haittaohjelma, joka leviää verkoissa ilman ihmisen toimia. (4 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

Etsi ruudukosta 8 piilotettua keskeistä sanastotermiä. Sanat voivat olla vaaka-, pysty- tai vinosuunnassa.

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

SANASTOLISTA

TROIJALAINEN LUNNASOHJELMA VAKOILUOHJELMA ROOTKIT HIEKKALAATIKKO
ERISTÄMINEN MATO TIEDOSTOTON

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

Yhdistä kukin sanahaun 8 sanastotermistä sen oikeaan määritelmään kirjoittamalla kirjain (A–H) tyhjään kohtaan.

SANASTOTERMIT

- **A. TROIJALAINEN**
- **B. LUNNASOHJELMA**
- **C. VAKOILUOHJELMA**
- **D. ROOTKIT**
- **E. HIEKKALAATIKKO**
- **F. ERISTÄMINEN**
- **G. MATO**
- **H. TIEDOSTOTON**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Piilottelun hallitseva haittaohjelma, joka piiloutuu syvälle järjestelmän ytimeen säilyttääkseen ylläpitäjän hallinnan.
2. Tartunnan saaneiden päätepisteiden rajoittaminen uhkien hyötykuormien leviämisen estämiseksi.
3. Haittaohjelma, joka suoritetaan suoraan RAM-muistissa levyskannereiden havaitsemisen välttämiseksi.
4. Itseään kopioiva haittaohjelma, joka leviää verkoissa ilman ihmisen toimia.
5. Haittaohjelma, joka salaa järjestelmän tallennustilan ja vaatii maksua avaimen toimittamisesta.
6. Ohjelma, joka on suunniteltu salaa seuraamaan ja tallentamaan käyttäjän toimia ja syötteitä.
7. Haitallinen ohjelma, joka on naamioitu harmittomaksi tai hyödylliseksi apuohjelmaksi.
8. Eristetty virtuaaliympäristö, jossa haitallisia tiedostoja analysoidaan turvallisesti.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

Selvitä alla olevat kirjaimet paljastaaksesi keskeisiä kyberturvallisuuden käsitteitä ja termejä. Kirjoita vastauksesi annettuihin syöttökenttiin.

1. IAAJRLNTEONI
2. IALKUMVLOAJEHO
3. HAIKAOTIELKAKK
4. OTMA
5. JLUNHAASEOLMN
6. IOKRTTO
7. ITERMNNEIÄS
8. TTNSETOIOOD

Bonustehtävä: Nopeat vastaukset

3 VASTAUSTA JOKAISEEN LUOKKAAN. VOITTAJA ON SE, JOKA TÄYTTÄÄ LISTAN ENSIMMÄISENÄ.

1	Paikkoja, joista ladata turvallisia sovelluksia			
2	Laitteita, jotka voidaan hakkeroida			
3	Asioita, joista otat varmuuskopion			
4	Varoitusmerkkejä sähköpostissa			
5	Merkkejä siitä, että puhelimessa on haittaohjelma			
6	Haittaohjelmatyyppejä, jotka tunnet			
7	Tiedostotyyppejä, joiden kanssa kannattaa olla varovainen			
8	Tapoja, joilla haittaohjelma pääsee tietokoneelle			
9	Turvallisia tapoja, joita voit aloittaa tänään			
10	Kyberturvallisuuteen liittyviä sanoja			
11	Asioita, joita teet tietovuodon jälkeen			
12	Syitä päivittää ohjelmistot			
13	Eläimiä tai hahmoja, joilla on haittaohjelmamaisia nimiä			
14	Asioita, joita haittaohjelma voi varastaa			
15	Asioita, joita teet, jos napsautit väärää linkkiä			

Tarkistuspiste 8: Kyberturvallisuuden tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: YRITYKSEN LUNNASOHJELMAN HYÖTYKUORMAN ERISTÄMINEN

👷

Tilanne: Yrityksen paikallisverkkoon on murtauduttu aktiivisella kiristyshaittaohjelmalla. Keskeisten tiedostopalvelimien tiedostopäätteiksi on alkanut tulla .locked. Laadi rajaamiskäytännöt.

Keskustelukysymys: Kuvaa eristysvaiheet yksityiskohtaisesti ja esitä tietojen palautusprotokolla.

TAPAUSTUTKIMUS 2: TIEDOSTOTTOMAN HAITTAOHJELMAN MUISTIINJEKTIO

👷

Tilanne: Analyytikko havaitsee epäilyttäviä skriptimalleja, jotka suoritetaan suoraan järjestelmän haihtuvassa RAM-muistissa tavallisilla ylläpitotyökaluilla, mutta levyllä ei ole haitallisia tiedostoja.

Keskustelukysymys: Selitä muistianalyysistrategia ja määritä työkalut tiedostottoman suorituksen estämiseksi.

Tarkistuspiste 9: Salakirjoituksen purkaminen

Kyberturvallisuuden ammattilainen suojaa verkon resursseja verkkohyökkääjiltä. Käytä alla olevaa kirjain–numero-avainta purkaaksesi viestin kirjoittamalla vastaavat kirjaimet tyhjiin kohtiin.

KIRJAIN-NUMERO-SALAUSAVAIN

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 Å=27 Ä=28 Ö=29

8	1	22	1	9	20	19	5		21	8	1	20

11	28	25	20	29	19	22	1	12	22	15	14	14	1	12	12	1

Purettu viesti:

VIHJE: JOKAINEN NUMERO VASTAA KIRJAIMEN PAIKKAA AAKKOSISSA (ESIM. 1 = A, 2 = B, 29 = Ö).

Tarkistuspiste 10: Usein kysytyt kysymykset kyberturvallisuudesta, perustaso (Osa A)

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q1: Mitä on haittaohjelma?

Uhkatoimijoiden suunnittelema haitallinen ohjelmisto, jonka tarkoitus on vahingoittaa laitteita ja verkkoja, kaapata niitä tai varastaa niistä tietoja.

Q2: Mikä ero on virukselle ja madolle?

Virus tarvitsee ihmisen toimia (kuten tiedoston avaamista) levitäkseen, kun taas mato leviää automaattisesti verkoissa.

Q3: Miten Troijan hevonen tartuttaa tietokoneen?

Se huijaa käyttäjiä esiintymällä vaarattomana tai turvallisena ohjelmana ja piilottaa haitallisen hyötykuormansa sisäänsä.

Q4: Mitä kiristyshaittaohjelma on?

Haittaohjelmatyyppi, joka salaa kohdejärjestelmän tiedostot ja vaatii rahallista maksua salauksenpurkuavaimesta. [1]

Q5: Mitä vakoiluohjelma on?

Haitallinen ohjelmisto, joka tallentaa salaa käyttäjän näppäilyt, salasanat ja selaustottumukset ja lähettää ne hyökkääjille.

Tarkistuspiste 10: Usein kysytyt kysymykset kyberturvallisuudesta, perustaso (Osa B)

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q6: Mitä hiekkalaatikointi tarkoittaa?

Epäilyttävien tiedostojen suorittaminen suojatussa, eristetyssä virtuaaliympäristössä niiden toiminnan havainnoimiseksi ilman riskiä tuotantojärjestelmille.

Q7: Mitä tiedostoton haittaohjelma on?

Haittaohjelma, joka toimii suoraan järjestelmämuistissa (RAM) laillisia apuohjelmia käyttäen eikä kirjoita tiedostoja levylle, jotta se ohittaisi yksinkertaiset tarkistimet.

Q8: Miten rootkit suojaa haittaohjelmaa?

Se piilottaa haitallisia prosesseja ja tiedostoja, usein horjuttamalla käyttöjärjestelmän ydintä, joten virustorjuntaskannerit voivat missata ne.

Q9: Mitä dynaaminen käyttäytymisen seuranta on?

Virustorjuntatarkistus, joka valvoo käynnissä olevia prosesseja reaaliajassa ja estää haittaohjelmille tyypillisiä toimia, kuten tiedostojen massasalauksen.

Q10: Miksi eristäminen on kiireellistä poikkeamiin reagoinnissa?

Vaarantuneiden päätelaitteiden eristäminen estää aktiivisten haittaohjelmien hyötykuormien leviämisen muihin verkon laitteisiin.

Tarkistuspiste 10: Usein kysytyt kysymykset tietoturvasta, jatkotaso (Osa C)

Tutustu tietoturvaviitekehysten, haittaohjelma-analyysin ja tietojen vaatimustenmukaisuuden edistyneisiin teknisiin puoliin.

Q1: Miten haittaohjelmien kehittäjät ohittavat allekirjoituspohjaiset virustorjuntaskannerit?

Ne käyttävät polymorfismia, joka muuttaa tiedoston tiivisteen ja koodirakenteen jokaisen tartunnan yhteydessä mutta säilyttää haitallisen toiminnan samana.

Q2: Mikä on kaksikäyttöisten työkalujen riski haittaohjelmakampanjoissa?

Hyökkääjät käyttävät lailliseksi tarkoitettuja ylläpitotyökaluja (kuten PowerShell tai Sysinternals) sulautuakseen tavalliseen verkkoliikenteeseen, mikä vaikeuttaa havaitsemista.

Q3: Miten process hollowing suorittaa haitallisia hyötykuormia?

Se käynnistää laillisen järjestelmäprosessin keskeytettynä, korvaa sen muistikoodin haittaohjelmalla ja jatkaa suoritusta.

Q4: Mikä on komento- ja hallintapalvelimen (C2) rooli?

Hakkereiden ylläpitämä etäpalvelin, joka lähettää ohjeita ja hyötykuormia kaapatuilla koneilla pyörivälle haittaohjelmalle.

Q5: Miksi näppäinten kaappausta on vaikea havaita?

Yksinkertaiset näppäinseurantaohjelmat kuluttavat vain vähän suoritinresursseja ja piilottavat prosessinsa laillisiin käyttäjätilan apuohjelmiin.

Tarkistuspiste 10: Usein kysytyt kysymykset tietoturvasta, jatkotaso (Osa D)

Tutustu tietoturvaviitekehysten, haittaohjelma-analyysin ja tietojen vaatimustenmukaisuuden edistyneisiin teknisiin puoliin.

Q6: Miten koodin obfuskointi hidastaa haittaohjelmien analyysiä?

Se salaa tai järjestelee lähdekoodin uudelleen, jolloin se on lukukelvotonta analyysityökaluille ja tietoturvaskannereille.

Q7: Mikä on bootkitin tehtävä?

Rootkit, joka tartuttaa käynnistysprosessin (MBR:n, käynnistyslohkon tai UEFI-laiteohjelmiston), joten se suoritetaan ennen käyttöjärjestelmän latautumista.

Q8: Miten heuristinen tarkistus tunnistaa nollapäivähaavoittuvuudet?

Se skannaa epäilyttäviä koodikuvioita ja hallintakomentoja sen sijaan, että etsisi vastaavaa tietokannan tiivistettä.

Q9: Mikä on DLL-kaappauksen uhka?

Oikeutetun sovelluksen pakottaminen lataamaan haitallinen dynaaminen linkkikirjasto (DLL) sijoittamalla se sovelluksen hakemistopolkuun.

Q10: Miten automaattiset haittaohjelma-analyysiputket hyödyntävät virtualisointia?

Ne ajavat epäilyttäviä tiedostoja usean käyttöjärjestelmän virtuaalikoneessa ja luovat automaattisesti toimintalokit ja verkon PCAP-tiedostot.

Osa 11: 10 tosielämän kyberturvallisuusfaktaa ja havaintoa

Tutustu todellisiin tosiasioihin tietoturvaloukkauksista, puolustusmekanismeista ja vaatimustenmukaisuusstandardeista.

1. TURVALLISUUSOIVALLUS

Troijalaiset ovat edelleen yleinen tartuntatapa, koska ne piilottavat haitallisen koodin harmittomilta näyttäviin ohjelmiin.

2. TURVALLISUUSOIVALLUS

FBI:n IC3 vastaanotti vuonna 2025 yli 3 600 kiristyshaittaohjelmaa koskevaa valitusta, ja ilmoitetut tappiot ylittivät 32 miljoonaa dollaria. [3]

3. TURVALLISUUSOIVALLUS

Madot voivat levitä nopeasti verkoissa hyödyntämällä korjaamattomia protokollahaavoittuvuuksia, kuten SMB:n EternalBluea.

4. TURVALLISUUSOIVALLUS

Tiedostotonta haittaohjelmaa on vaikea havaita, koska se toimii muistissa laillisten työkalujen kautta ja jättää levylle vain vähän jälkiä.

5. TURVALLISUUSOIVALLUS

Analyysihiekkalaatikot palautuvat tyypillisesti puhtaaseen tilannekuvaan jokaisen ajon jälkeen, jotta jokainen testi alkaa tunnetusta tilasta.

6. TURVALLISUUSOIVALLUS

Rootkitit voivat muokata ytimen järjestelmäkutsuja ja raportoida vääriä diagnostiikkatuloksia haittaohjelmatarkistimille.

7. TIETOTURVATIETOA

Koodin hämäys käyttää pakkausohjelmia haittaohjelman todellisen binäärihyötykuorman rakenteen pakkaamiseen ja piilottamiseen.

8. TIETOTURVATIETOA

Polymorfinen haittaohjelma muuttaa koodiaan ja siten tiedostotiivisteensä jokaisessa uudessa kopiossa väistääkseen allekirjoitustarkistukset.

9. TIETOTURVATIETOA

DLL-kaappaus hyödyntää hakujärjestyksen asetuksia tavallisissa käyttöjärjestelmissä, kuten Windowsissa.

10. TURVALLISUUSOIVALLUS

Tietoturvatoimittajat löytävät päivittäin valtavia määriä uusia haittaohjelmanäytteitä, joten allekirjoituksia on päivitettävä jatkuvasti.

Tekniset viitteet ja lähteet

Opiskeluopas ja interaktiiviset pulmat on koottu maailmanlaajuisista NIST-, OWASP- ja tietosuojavaatimustenmukaisuusstandardeista.

TIETEELLISET JA ALAN VIITTEET

[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

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 Kysymys 1

Oikea vastaus: A

OPETTAJALLE

Mikä on troijalaisen määrittävä ominaisuus? → Se esiintyy aitona ohjelmistona huijatakseen käyttäjiä suorittamaan sen

2 Kysymys 2

Oikea vastaus: A

OPETTAJALLE

Minkä tyyppinen haittaohjelma salaa tiedostot ja vaatii maksua? → Kiristyshaittaohjelma

3 Kysymys 3

Oikea vastaus: A

OPETTAJALLE

Mikä edustaa vakoiluohjelmaa? → Haittaohjelma, joka on suunniteltu seuraamaan salaa käyttäjän näppäilyjä ja selaintoimintaa

4 Kysymys 4

Oikea vastaus: A

OPETTAJALLE

Miksi haittaohjelmakehittäjät käyttävät rootkit-ohjelmia? → Piilottaa aktiiviset prosessit ja haitalliset tiedostot käyttöjärjestelmältä

5 Kysymys 5

Oikea vastaus: A

OPETTAJALLE

Mitä hiekkalaatikkoeristys (sandboxing) tarkoittaa haittaohjelma-analyysissa? → Epäilyttävien tiedostojen suorittaminen eristetyssä virtuaalisessa holvissa käyttäytymisen turvalliseksi tarkkailemiseksi

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Kysymys 6** — **Oikea vastaus: Epätosi**

OPETTAJALLE

Epätosi: madot kopioituvat itsestään ja leviävät verkoissa ilman käyttäjän toimia.

7 **Kysymys 7** — **Oikea vastaus: Epätosi**

OPETTAJALLE

Epätosi: mainosohjelmat eivät aina ole vaarattomia; suuri osa seuraa selailua mainosten kohdentamiseksi.

8 **Kysymys 8** — **Oikea vastaus: Tosi**

OPETTAJALLE

Tosi: puhtaat offline-varmuuskopiot palauttavat salatut tiedostot maksamatta, vaikka varastetut tiedot voivat silti vuotaa.

9 **Kysymys 9** — **Oikea vastaus: Epätosi**

OPETTAJALLE

Epätosi: allekirjoitusskannerit tarvitsevat tunnetun näytteen, joten aivan uusi nollapäivähaittaohjelma voi livahtaa niiden ohi.

10 **Kysymys 10** — **Oikea vastaus: Tosi**

OPETTAJALLE

Tiedostoton haittaohjelma suorittaa haitallisia skriptejä järjestelmämuistissa välttäen tiedostojen kirjoittamista levylle.

Sanastoavaimet ja arviointikriteerit

Opettajan arviointikriteeri: Anna 1 piste jokaisesta oikeasta yhdistämisestä (yhteensä 8 pistettä) ja asiayhteystermistä (yhteensä 6 pistettä).

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

D 1. TROJALAINEN	F 2. KIRISTYSHAITTAOHJELMA	A 3. VAKOILUOHJELMA	H 4. ROOTKIT
G 5. HIEKKALAATIKKO	C 6. ERISTÄMINEN	E 7. MATO	B 8. TIEDOSTOTON

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 TROIJALAINEN	2 LUNNASOHJELMA	3 VAKOILUOHJELMA	4 ROOTKIT
5 HIEKKALAATIKKO	6 ERISTÄMINEN		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 D – ROOTKIT	2 F – ERISTÄMINEN	3 H – TIEDOSTOTON	4 G – MATO
5 B – LUNNASOHJELMA	6 C – VAKOILUOHJELMA	7 A – TROIJALAINEN	8 E – HIEKKALAATIKKO

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit TROJALAINEN, KIRISTYSHAITTAOHJELMA ja VAKOILUOHJELMA omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

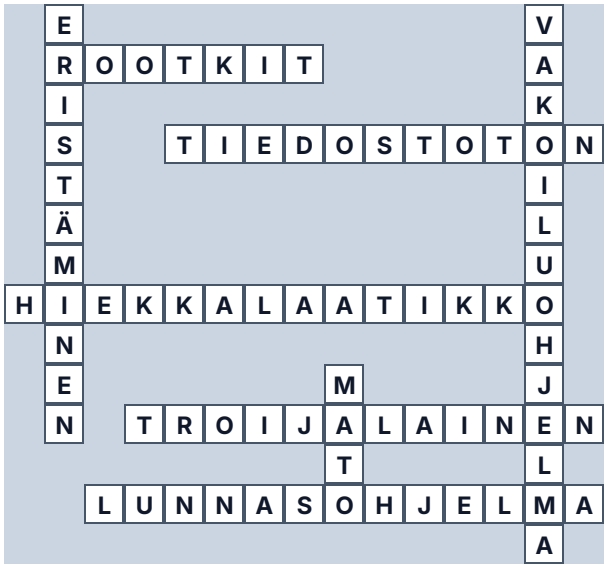
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

3 vaakasuoraan: ROOTKIT Piilottelun hallitseva haittaohjelma, joka piiloutuu syvälle järjestelmän ytimeen säilyttääkseen ylläpitäjän hallinnan. (7 kirjainta)

4 vaakasuoraan: TIEDOSTOTON Haittaohjelma, joka suoritetaan suoraan RAM-muistissa levyskannereiden havaitsemisen välttämiseksi. (11 kirjainta)

5 vaakasuoraan: HIEKKALAATIKKO Eristetty virtuaaliympäristö, jossa haitallisia tiedostoja analysoidaan turvallisesti. (14 kirjainta)

7 vaakasuoraan: TROIJALAINEN Haitallinen ohjelma, joka on naamioitu harmittomaksi tai hyödylliseksi apuohjelmaksi. (12 kirjainta)

8 vaakasuoraan: LUNNASOHJELMA Haittaohjelma, joka salaa järjestelmän tallennustilan ja vaatii maksua avaimen toimittamisesta. (13 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: ERISTÄMINEN Tartunnan saaneiden päätepisteiden rajoittaminen uhkien hyötykuormien leviämisen estämiseksi. (11 kirjainta)

2 pystysuoraan: VAKOILUOHJELMA Ohjelma, joka on suunniteltu salaa seuraamaan ja tallentamaan käyttäjän toimia ja syötteitä. (14 kirjainta)

6 pystysuoraan: MATO Itseään kopioiva haittaohjelma, joka leviää verkoissa ilman ihmisen toimia. (4 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. I A A J R L N T E O N I — **TROIJALAINEN**
2. I A L K U M V L O A J E H O — **VAKOILUOHJELMA**
3. H A I K A O T I E L K A K K — **HIEKKALAATIKKO**
4. O T M A — **MATO**
5. J L U N H A A S E O L M N — **LUNNASOHJELMA**
6. I O K R T T O — **ROOTKIT**
7. I T E R M N N E I Ä S — **ERISTÄMINEN**
8. T T N S E T O I O O D — **TIEDOSTOTON**

SALAKIRJOITUSHAASTEEN AVAIN

"HAVAITSE UHAT KÄYTÖSVALVONNALLA"

Tapaustutkimusten vastausavain

A Tapaustutkimus 1: Yrityksen lunnasohjelman hyötykuorman eristäminen

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Yrityksen lähiverkkoon on murtauduttu aktiivisella kiristysohjelmalla. Keskeisten tiedostopalvelimien tiedostopäätteiksi on alkanut tulla .locked. Laadi rajaamiskäytännöt.
- Suositeltu strategia ja ratkaisu: Irrota kaikki vaikutuksen alaiset palvelimet lähiverkosta. Katkaise aktiiviset ylläpitoistunnot. Palauta puhtaat tiedostot suojatusta, kirjoitussuojatusta offline-varmuuskopiojärjestelmästä.

B Tapaustutkimus 2: Tiedostottoman haittaohjelman muistiinjektio

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Analyytikko havaitsee epäilyttäviä skriptauskuvioita, jotka suoritetaan suoraan haihtuvassa järjestelmän RAM-muistissa tavallisilla hallintatyökaluilla, mutta levyllä ei ole haitallisia tiedostoja.
- Suositeltu strategia ja ratkaisu: Eristä vaikutuksen kohteena olevat päätelaitteet ja ota ensin muistivedos. Tarkista PowerShell- ja WMI-lokit, estä hyväksymättömät skriptit AppLockerilla ja käynnistä sitten uudelleen haittakuorman poistamiseksi.