Nimi: _____ Päivämäärä: _____ Pisteet: _____

Kiristyshaittaohjelmahyökkäykset ja liiketoiminta Palautus

Haittakuorman suoritus, tiedostojen salaus, offline-varmuuskopiot, eristystoimet ja katastrofista toipuminen.

KIRISTYSHAITTAOHJELMAHYÖKKÄYSTEN OPPIMISKATSAUS

SUOJATTU
TIETOJEN SALAUS
256-bittinen AES-standardi

LAINMUKAINEN
GLOBAALIT STANDARDIT
GDPR- ja CCPA-säädökset

NOLLALUOTTAMUS
KÄYTTÖKÄYTÄNTÖ
Monivaiheinen tunnistautuminen

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: kiristysohjelmahyökkäykset ja liiketoiminnan palautuminen. Tutustut haittakuorman suorittamiseen, tiedostojen salaukseen, offline-varmuuskopioihin, uhkien eristämiseen, kryptovaluuttamaksuihin ja katastrofipalautussuunnitelmiin.

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/ransomware-hyokkays/

Oppimispolkusi: kiristysohjelmasta toipuminen

- Erota toisistaan troijalaisten, kiristysohjelmien ja vakoiluohjelmien hyötykuormat.
- Analysoi haitallisia tiedostoja suojatuissa hiekkalaatikkoympäristöissä.
- Laadi nopeat verkon eristämis- ja rajaamismenettelyt.

KIRISTYSHAITTAOHJELMAHYÖKKÄYSTEN OPAS

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

KIRISTYSHAITTAOHJELMAHYÖKKÄYKSET JA PALAUTUMINEN KATASTROFEISTA (JOHDANTO)

Kiristyshaittaohjelman hyötykuormat lukitsevat järjestelmän tallennustilan salauksella ja vaativat kryptovaluuttamaksuja salauksenpurkuavaimista. Uhkaa voidaan lieventää verkon eristyssäännöillä, hiekkalaatikossa tehtävällä haittaohjelma-analyysillä ja vankoilla ilmaerotetuilla kylmävarmuuskopioilla.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. Mikä on kiristysohjelmahyökkäyksen ensisijainen toimintamekanismi?

- A. Käyttäjän tiedostojen salaus järjestelmän käytön estämiseksi
- B. Haitallisten SQL-komentojen syöttäminen lomakekenttiin
- C. Verkkopakettien nuuskiminen julkisessa Wi-Fi-yhteydessä
- D. Sähköpostiotsikoiden väärentäminen SPF-validoinnin ohittamiseksi

2. Mikä on offline-varmuuskopio (kylmä varmuuskopio)?

- A. Verkosta irrotettu tallennuskopio, joka suojaa sen haittaohjelmien leviämiseltä
- B. Varmuuskopio, joka on tallennettu ensisijaisen verkkopalvelimen kiintolevylle
- C. Järjestelmän rekisterilokien väliaikainen välimuisti
- D. Ylläpitotyökalu, jolla nollataan käyttäjien salasanoja

3. Miten tietoturvatiimien tulisi eristää tartunnan saaneet järjestelmät kiristysohjelmahyökkäyksen aikana?

- A. Irrota verkkokaapelit ja poista langattomat liittymät käytöstä välittömästi
- B. Päivitä virustorjunnan allekirjoitustietokanta
- C. Sammuta ensisijainen DNS-palvelin
- D. Nimeä vaarantuneiden tiedostojen päätteet uudelleen

4. Miksi turvallisuusviranomaiset neuvovat olemaan maksamatta kiristysohjelmien vaatimuksia?

- A. Maksaminen rohkaisee hyökkääjiä eikä takaa salauksenpurkuavaimen toimitusta
- B. Se mitätöi automaattisesti kaikki yrityksen vakuutukset
- C. Se ilmoittaa automaattisesti jokaiselle asiakkaalle sähköpostilla
- D. Se turmelee jäljellä olevat järjestelmän varmuuskopiotiedostot

5. Mikä on palautumissuunnitelma (DRP)?

- A. Jäsennelty prosessi toiminnan ja tietojen palauttamiseksi järjestelmän vaarantumisen jälkeen
- B. Palomuurin määritys, joka yhdistää saapuvat verkkoportit
- C. Tietokantaskeema, jossa luetellaan käyttäjien hallinnolliset oikeudet
- D. Sähköpostin todennusprotokolla, joka hylkää väärennetyt verkkotunnukset

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Kiristyshaittaohjelman hyötykuormat voivat levitä helposti verkkoon liitettyihin verkossa oleviin varmuuskopioihin.

- ◯ Tosi
- ◯ Epätosi

7 Kysymys 7

7. Kryptovaluuttana maksettu lunnasmaksu takaa, että tiedostot palautuvat onnistuneesti.

- ◯ Tosi
- ◯ Epätosi

8 Kysymys 8

8. Tartunnan saaneiden järjestelmien irrottaminen verkosta auttaa estämään kiristyshaittaohjelman leviämisen viereisiin järjestelmiin.

- ◯ Tosi
- ◯ Epätosi

9 Kysymys 9

9. Kiristyshaittaohjelmat eivät koskaan käytä symmetristä kryptografiaa järjestelmän tallennustilan salaamiseen.

- ◯ Tosi
- ◯ Epätosi

10 Kysymys 10

10. Tietojen palautusmenettelyjen säännöllinen testaus on keskeinen osa katastrofipalautusta.

- ◯ Tosi
- ◯ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Paikallisten tiedostojen käytön estää kryptografinen _____ .
2. Järjestelmässä suoritettava aktiivinen haitallinen koodi on _____ .
3. Verkosta irrotetut ulkopuolisen tallennuksen kopiot ovat turvallinen _____ .
4. Haittaohjelman leviämisen pysäyttämiseksi tarvitaan päätepisteen verkkoyhteyden katkaisu eli _____ .
5. Kyberrikollisten vaatimat kryptovaluuttamaksut ovat _____ .
6. Toiminnallisten datatiedostojen palauttaminen on katastrofin jälkeinen _____ .

SANASTON SANAPANKKI

ERISTYS | HYÖTYKUORMA | KATASTROFI | LUNNAAT | OFFLINE-KOPIO | PALAUTUS | SALAUS | TROIJALAINEN

Kirjoita vastauksesi tähän:

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

Tarkistuspiste 4: Tietoturvakäsitteiden yhdistäminen

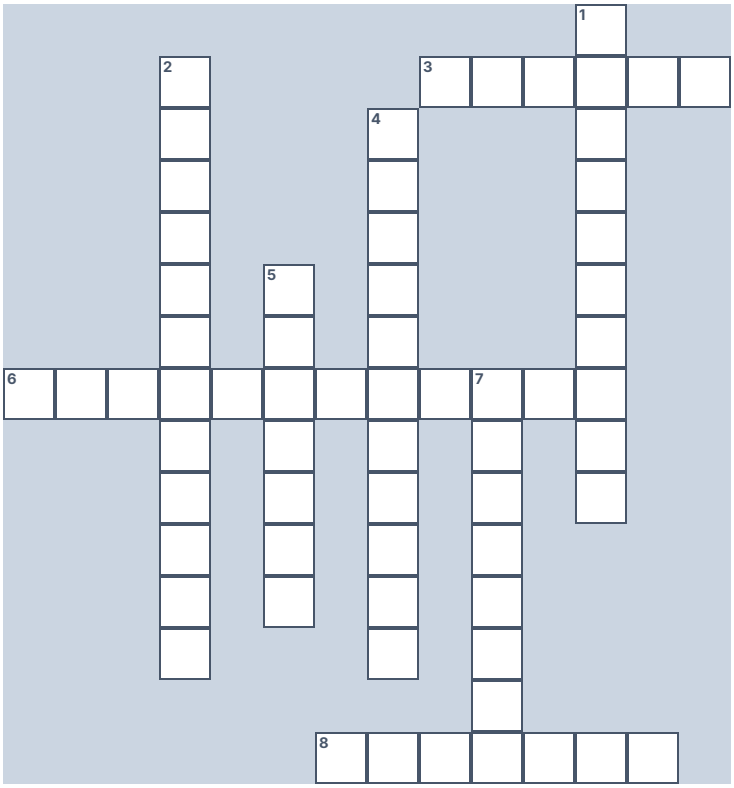
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. SALAUS	A	Tartunnan saaneiden verkkojärjestelmien irrottaminen.
☐	2. KUORMA	B	Haitallinen tiedosto, joka on naamioitu vaarattomaksi.
☐	3. KYLMÄVARMUUSKOPIO	C	Tiedostojen lukitseminen salausmenetelmin.
☐	4. ERISTYS	D	Suuri järjestelmähäiriö.
☐	5. LUNNAAT	E	Haitallisen ohjelmiston suorittaminen.
☐	6. PALAUTUS	F	Irrotettu offline-kopio.
☐	7. KATASTROFI	G	Tietokannan palauttaminen varmuuskopiosta.
☐	8. TROJALAINEN	H	Kryptografisen avaimen palautuspyyntö.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

3. Tiedostojen lukitseminen kryptografisesti. (6)

6. Irrotettu, verkosta erillään oleva kopio. (12)

8. Tartunnan saaneiden verkkojärjestelmien irrottaminen. (7)

PYSTYSUORAAN

1. Merkittävä järjestelmän häiriötilanne. (10)

2. Puhtaaksi naamioitu haitallinen tiedosto. (12)

4. Haitallisen ohjelmiston suorittaminen. (11)

5. Kryptografisen avaimen lunastuspyyntö. (7)

7. Tietokannan palauttaminen varmuuskopiosta. (8)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

3 vaakasuoraan: Tiedostojen lukitseminen kryptografisesti. (6 kirjainta):

6 vaakasuoraan: Irrotettu, verkosta erillään oleva kopio. (12 kirjainta):

8 vaakasuoraan: Tartunnan saaneiden verkkojärjestelmien irrottaminen. (7 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Merkittävä järjestelmän häiriötilanne. (10 kirjainta):

2 pystysuoraan: Puhtaaksi naamioitu haitallinen tiedosto. (12 kirjainta):

4 pystysuoraan: Haitallisen ohjelmiston suorittaminen. (11 kirjainta):

5 pystysuoraan: Kryptografisen avaimen lunastuspyyntö. (7 kirjainta):

7 pystysuoraan: Tietokannan palauttaminen varmuuskopiosta. (8 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

SALAUS HYÖTYKUORMA OFFLINEKOPIO ERISTYS LUNNAAT PALAUTUS KATASTROFI TROIJALAINEN

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. SALAUS**
- **B. HYÖTYKUORMA**
- **C. OFFLINEKOPIO**
- **D. ERISTYS**
- **E. LUNNAAT**
- **F. PALAUTUS**
- **G. KATASTROFI**
- **H. TROIJALAINEN**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Irrotettu, verkosta erillään oleva kopio.
2. Puhtaaksi naamioitu haitallinen tiedosto.
3. Tiedostojen lukitseminen kryptografisesti.
4. Kryptografisen avaimen lunastuspyyntö.
5. Tartunnan saaneiden verkkojärjestelmien irrottaminen.
6. Merkittävä järjestelmän häiriötilanne.
7. Haitallisen ohjelmiston suorittaminen.
8. Tietokannan palauttaminen varmuuskopiosta.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. LSAUSA
2. OFINOPIFKOEL
3. NLATNAU
4. TFSIAORKAT
5. RYOUÖAYKHMT
6. YITESSR
7. PSUTUAAL
8. AOJNLNTAREII

Bonustehtävä: Nopeat vastaukset

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

1	Tietoja, joita sinun ei pitäisi koskaan jakaa			
2	Laitteita, jotka voidaan hakkeroida			
3	Syitä olla maksamatta lunnaita			
4	Turvallisia tapoja, joita voit aloittaa tänään			
5	Tietoturvatyökaluja, jotka tunnet			
6	Tapoja suojata tilisi			
7	Merkkejä siitä, että tietokone on saanut tartunnan			
8	Paikkoja varmuuskopion säilyttämiseen			
9	Tiedostoja, joita et halua koskaan menettää			
10	Tapoja, joilla kiristyshaittaohjelma leviää			
11	Asioita, joita teet hyökkäyksen ensimmäisellä tunnilla			
12	Ihmisiä, joihin otat yhteyttä hyökkäyksen aikana			
13	Asioita, jotka kiristyshaittaohjelma voi lukita			
14	Kyberturvallisuuteen liittyviä sanoja			
15	Organisaatioita, joihin hyökätään usein			

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.

Keskustelukysymys: Kuvaa eristysvaiheet yksityiskohtaisesti ja esitä tietojen palautusprotokolla.

TAPAUSTUTKIMUS 2: OFFLINE-VARMUUSKOPIOARKKITEHTUURIEN ARVIOINTI

👷

Tilanne: Yritys haluaa suunnitella tietojen varmuuskopiointistrategian, joka pienentää riskiä, että varmuuskopiot vaarantuvat, vaikka ensisijainen paikallisverkko olisi kokonaan kiristyshaittaohjelman kaappaama.

Keskustelukysymys: Suunnittele suojattu offline-varmuuskopioiden tallennusholvi.

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

16	1	12	1	21	20	1		19	1	12	1	20	21	20

20	9	5	4	15	20		11	25	12	13	28	19	20	28

11	15	16	9	15	19	20	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: Mikä on kiristysohjelma?

Kiristyshaittaohjelma on haittaohjelmisto, joka on suunniteltu estämään pääsy tietokonejärjestelmiin tai tiedostoihin, kunnes lunnaat on maksettu.

Q2: Miten kiristysohjelma leviää?

Tietojenkalasteluviestien liitteiden, korjaamattomien ohjelmistohaavoittuvuuksien ja vaarantuneiden etäkäyttöjärjestelmien kautta. [1]

Q3: Miksi maksua pyydetään kryptovaluutalla?

Bitcoinin kaltaiset kryptovaluutat tarjoavat suhteellista anonyymiyttä, mikä vaikeuttaa varojen jäljittämistä lainvalvonnalle.

Q4: Estääkö virustorjunta kiristyshaittaohjelmat?

Kyllä, mutta allekirjoituspohjainen virustorjunta voi epäonnistua uusia nollapäivän kiristysohjelmien hyötykuormia vastaan.

Q5: Mikä on ilmaerotettu varmuuskopio?

Varmuuskopio, jolla ei ole fyysistä tai loogista yhteyttä ensisijaiseen verkkoon, mikä suojaa sitä leviämiseltä.

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

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q6: Mitä kaksinkertainen kiristys on?

Kun hyökkääjät eivät vain salaa tiedostoja vaan myös varastavat arkaluonteisia tietoja ja uhkaavat vuotaa ne julkisiksi, jos lunnaita ei makseta.

Q7: Mikä on purkuohjelma?

Ohjelmistotyökalu, joka sisältää salausavaimen, jota tarvitaan lukittujen tiedostojen palauttamiseen selkokielelle.

Q8: Miten kiristyshaittaohjelma havaitaan varhain?

Valvomalla tiedostojärjestelmiä äkillisen, massiivisen tiedostojen muokkaus- ja uudelleennimeämistoiminnan varalta.

Q9: Mikä rooli vakuutuksella on?

Kyberturvavakuutus voi auttaa kattamaan palautumiskustannuksia, mutta vakuutusehdot ja lunnaiden maksusäännöt vaihtelevat vakuutuskohtaisesti.

Q10: Pitäisikö tartunnan saanut järjestelmä käynnistää uudelleen?

Ei, uudelleenkäynnistys voi tuhota haihtuvan muistin todisteet; eristä se verkosta sen sijaan. [1]

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

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

Q1: Miten kiristysohjelma käyttää epäsymmetristä salausta?

Se käyttää haittaohjelmaan upotettua julkista avainta tiedostojen salaamiseen, ja purkamiseen tarvitaan hyökkääjän yksityinen avain.

Q2: Miksi käytetään myös symmetristä salausta?

Symmetrinen salaus (kuten AES) on nopea ja voi lukita valtavia tietokantoja minuuteissa, kun taas epäsymmetriset avaimet suojaavat AES-avaimen.

Q3: Mitä looginen segmentointi on?

Verkkojen jakaminen eristettyihin vyöhykkeisiin, mikä estää haittaohjelmaa leviämästä sivusuunnassa työasemista ydinpalvelimiin.

Q4: Mikä on WORM-tallennus?

Write-Once, Read-Many -tallennusväline, joka estää kiristysohjelmien hyötykuormia muokkaamasta, ylikirjoittamasta tai poistamasta varmuuskopiodataa.

Q5: Mitä varjokopiot ovat?

Windowsin luomat paikalliset varmuuskopiovedokset; kiristyshaittaohjelmat poistavat ne tyypillisesti ensimmäisenä ylläpitotyökaluilla.

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

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

Q6: Miten tunnistetietojen varkaus mahdollistaa kiristyshaittaohjelmat?

Hyökkääjät ostavat vuodettuja ylläpitäjien tunnuksia kirjautuakseen etätyöpöydillä ja suorittavat kiristysohjelman käsin koko verkossa.

Q7: Mitä koepalautustestaus on?

Varmuuskopiotietokantojen säännöllinen palauttaminen eristettyihin testiympäristöihin sen varmistamiseksi, että palautusnopeus ja tietojen eheys täyttävät katastrofipalautuksen mittarit.

Q8: Miten päätelaitteiden havaitseminen (EDR) pysäyttää kiristyshaittaohjelmat?

Analysoimalla prosessien toimintaa (esim. nopea salaus) ja keskeyttämällä nopeasti haitallinen sovellus.

Q9: Mikä on kiristyshaittaohjelma palveluna (RaaS) -malli?

Franchising-malli, jossa haittaohjelmakehittäjät vuokraavat kiristyshaittaohjelmien rakennustyökaluja kumppaneille vastineeksi osuudesta tuotoista.

Q10: Miten korjaamaton RDP laukaisee kiristysohjelman?

Altistuneet, päivittämättömät Remote Desktop Protocol -yhdyskäytävät antavat hyökkääjien murtaa kirjautumisia raa'alla voimalla ja käynnistää haittaohjelmia manuaalisesti.

Osa 11: 10 tosielämän kyberturvallisuusfaktaa ja havaintoa

Tutustu todellisiin tosiasioihin tietoturvaloukkauksista, puolustusmekanismeista ja vaatimustenmukaisuusstandardeista.

1. TURVALLISUUSOIVALLUS

Kiristyshaittaohjelmien tekijät käyttävät usein työkaluja, kuten vssadmin.exe, poistaakseen Windowsin varjokopiot ja estääkseen paikalliset palautukset. [1]

2. TURVALLISUUSOIVALLUS

Symmetrisiä AES-256-avaimia käytetään tyypillisesti tiedostojen hyötykuormien salaamiseen, jotka sitten lukitaan julkisilla RSA-avaimilla.

3. TURVALLISUUSOIVALLUS

Onnistuneesta kiristysohjelmahyökkäyksestä toipuminen voi kestää viikkoja, minkä vuoksi testatut offline-varmuuskopiot ovat tärkeitä.

4. TURVALLISUUSOIVALLUS

FBI ei kannata kiristysvaatimuksen maksamista ja varoittaa, ettei maksaminen takaa, että saat tietosi takaisin. [2]

5. TURVALLISUUSOIVALLUS

Palautumissuunnitelmien (DRP) tulisi määritellä palautusaikatavoite (RTO) ja palautuspistetavoite (RPO).

6. TURVALLISUUSOIVALLUS

FBI suosittelee salattuja ja muuttumattomia varmuuskopioita, joita ei voi muuttaa eikä poistaa. [3]

7. TIETOTURVATIETOA

Kiristyshaittaohjelmien kehittäjät käyttävät edistyneitä obfuskointitekniikoita ohittaakseen perinteiset allekirjoituspohjaiset virustorjuntatarkistimet.

8. TIETOTURVATIETOA

Verkon segmentointi rajoittaa sivuttaisliikettä ja auttaa estämään kiristyshaittaohjelman leviämisen ensimmäistä tartunnan saanutta isäntää pidemmälle. [3]

9. TIETOTURVATIETOA

Altistuneet, heikosti suojatut etäpalvelut, kuten Remote Desktop Protocol (RDP), ovat yleinen kiristysohjelmien sisääntulopiste. [1]

10. TURVALLISUUSOIVALLUS

CISA suosittelee pitämään salatut varmuuskopiot offline-tilassa, koska monet lunnasohjelmaversiot etsivät ja poistavat tavoitettavissa olevia varmuuskopioita. [1]

Tekniset viitteet ja lähteet

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

TIETEELLISET JA ALAN VIITTEET

[1] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-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 kiristysohjelmahyökkäyksen ensisijainen toimintamekanismi? → Käyttäjän tiedostojen salaus järjestelmän käytön estämiseksi

2 Kysymys 2

Oikea vastaus: A

OPETTAJALLE

Mikä on offline-varmuuskopio (kylmä varmuuskopio)? → Verkosta irrotettu tallennuskopio, joka suojaa sen haittaohjelmien leviämiseltä

3 Kysymys 3

Oikea vastaus: A

OPETTAJALLE

Miten tietoturvatiimien tulisi eristää tartunnan saaneet järjestelmät kiristysohjelmahyökkäyksen aikana? → Irrota verkkokaapelit ja poista langattomat liittymät käytöstä välittömästi

4 Kysymys 4

Oikea vastaus: A

OPETTAJALLE

Miksi turvallisuusviranomaiset neuvovat olemaan maksamatta kiristysohjelmien vaatimuksia? → Maksaminen rohkaisee hyökkääjiä eikä takaa salauksenpurkuavaimen toimitusta

5 Kysymys 5

Oikea vastaus: A

OPETTAJALLE

Mikä on palautumissuunnitelma (DRP)? → Jäsennelty prosessi toiminnan ja tietojen palauttamiseksi järjestelmän vaarantumisen jälkeen

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Kysymys 6** — **Oikea vastaus: Tosi**

OPETTAJALLE

Kiristyshaittaohjelman hyötykuormat voivat levitä helposti verkkoon liitettyihin verkossa oleviin varmuuskopioihin.

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

OPETTAJALLE

Epätosi: FBI varoittaa, että maksaminen ei takaa, että saat mitään dataa takaisin. [2]

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

OPETTAJALLE

Tosi: CISA neuvoo irrottamaan tartunnan saaneet isännät tai ottamaan verkon offline-tilaan leviämisen hillitsemiseksi.

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

OPETTAJALLE

Epätosi: kiristyshaittaohjelma salaa tiedostot yleensä nopeilla symmetrisillä salausalgoritmeilla, kuten AES:llä.

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

OPETTAJALLE

Tietojen palautusmenettelyjen säännöllinen testaus on keskeinen osa katastrofipalautusta.

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

C 1. SALAUS	E 2. KUORMA	F 3. KYLMÄVARMUUSKOPIO	A 4. ERISTYS
H 5. LUNNAAT	G 6. PALAUTUS	D 7. KATASTROFI	B 8. TROJALAINEN

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 SALAUS	2 HYÖTYKUORMA	3 OFFLINE-KOPIO	4 ERISTYS
5 LUNNAAT	6 PALAUTUS		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 C – OFFLINEKOPIO	2 H – TROIJALAINEN	3 A – SALAUS	4 E – LUNNAAT
5 D – ERISTYS	6 G – KATASTROFI	7 B – HYÖTYKUORMA	8 F – PALAUTUS

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit SALAUS, KUORMA ja KYLMÄVARMUUSKOPIO omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

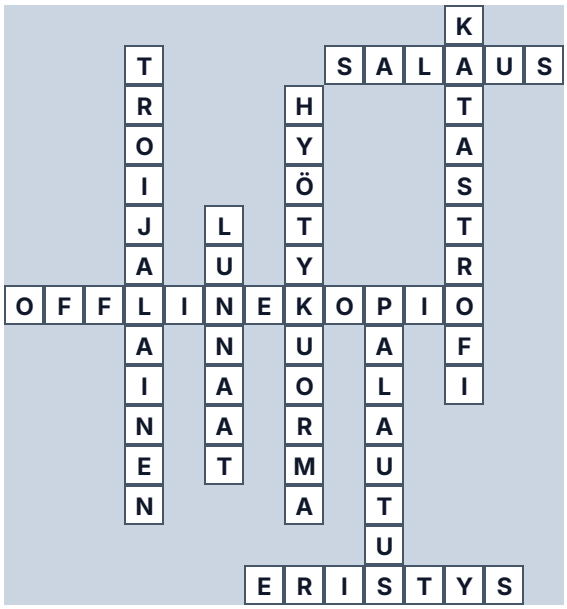
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

3 vaakasuoraan: SALAUS Tiedostojen lukitseminen kryptografisesti. (6 kirjainta)

6 vaakasuoraan: OFFLINEKOPIO Irrotettu, verkosta erillään oleva kopio. (12 kirjainta)

8 vaakasuoraan: ERISTYS Tartunnan saaneiden verkkojärjestelmien irrottaminen. (7 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: KATASTROFI Merkittävä järjestelmän häiriötilanne. (10 kirjainta)

2 pystysuoraan: TROIJALAINEN Puhtaaksi naamioitu haitallinen tiedosto. (12 kirjainta)

4 pystysuoraan: HYÖTYKUORMA Haitallisen ohjelmiston suorittaminen. (11 kirjainta)

5 pystysuoraan: LUNNAAT Kryptografisen avaimen lunastuspyyntö. (7 kirjainta)

7 pystysuoraan: PALAUTUS Tietokannan palauttaminen varmuuskopiosta. (8 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. LSAUSA — **SALAUS**
2. OFINOPIFKOEL — **OFFLINEKOPIO**
3. NLATNAU — **LUNNAAT**
4. TFSIAORKAT — **KATASTROFI**
5. RYOUÖAYKHMT — **HYÖTYKUORMA**
6. YITESSR — **ERISTYS**
7. PSUTUAAL — **PALAUTUS**
8. AOJNLNTAREII — **TROIJALAINEN**

SALAKIRJOITUSHAASTEEN AVAIN

"PALAUTA SALATUT TIEDOT KYLMÄSTÄ KOPIOSTA"

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.
- Suositeltu strategia ja ratkaisu: Irrota kaikki vaikutuksen alaiset palvelimet lähiverkosta. Katkaise aktiiviset ylläpitoistunnot. Palauta puhtaat tiedostot suojatusta, kirjoitussuojatusta offline-varmuuskopiojärjestelmästä.

B Tapaustutkimus 2: Offline-varmuuskopioarkkitehtuurien arviointi

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Yritys haluaa suunnitella tietojen varmuuskopiointistrategian, joka pienentää riskiä varmuuskopioiden vaarantumisesta, vaikka kiristyshaittaohjelma kaappaisi ensisijaisen paikallisverkon täysin.
- Suositeltu strategia ja ratkaisu: Ota käyttöön kertakirjoitteinen WORM-tallennus (write-once-read-many). Muodosta looginen ilmaväli katkaisemalla varmuuskopiojärjestelmä kaikista verkoista ja pakota päivittäinen fyysisen median kierrätys.