EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISAN THREAT LANDSCAPE - RAPORTTI 2021

Huhtikuusta 2020 heinäkuun 2021 puoliväliin

LOKAKUU 2021

TIETOA ENISASTA

Euroopan unionin kyberturvallisuusvirasto, ENISA, on unionin virasto, jonka tarkoituksena on saavuttaa yhteinen korkea kyberturvataso koko EU:ssa. Virasto perustettiin vuonna 2004, ja sitä on myöhemmin vahvistettu EU:n kyberturvallisuusasetuksella. Euroopan unionin kyberturvallisuusvirasto osallistuu EU:n kyberpolitiikan laatimiseen, edistää tieto- ja viestintäteknisten tuotteiden, palvelujen ja prosessien luotettavuutta kyberturvallisuuden sertifiointijärjestelmillä, tekee yhteistyötä jäsenvaltioiden ja EU:n elinten kanssa sekä auttaa EU:ta valmistautumaan tulevaisuuden kyberhaasteisiin. Virasto jakaa tietämystä, kehittää valmiuksia ja lisää tietoisuutta sekä tekee yhteistyötä keskeisten sidosryhmiensä kanssa lujittaakseen luottamusta verkottuneeseen talouteen, parantaakseen unionin infrastruktuurin sietokykyä ja ennen kaikkea suojatakseen eurooppalaisen yhteiskunnan ja kansalaisten digitaalista turvallisuutta. ENISAsta ja sen työstä on lisätietoa osoitteessa www.enisa.europa.eu.

OTA YHTEYTTÄ

Ota yhteyttä tekijöihin sähköpostilla etl@enisa.europa.eu.
Tätä asiakirjaa koskevat tiedotusvälineiden tiedustelut sähköpostilla press@enisa.europa.eu.

TOIMITTAJAT

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – Euroopan unionin kyberturvallisuusvirasto

MUUT OSALLISTUJAT

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

KIITOKSET

Haluamme kiittää ENISAn kyberuhkia käsittelevän tilapäisen työryhmän jäseniä ja tarkkailijoita arvokkaasta palautteesta ja kommenteista tämän raportin viimeistelyssä. Haluamme myös kiittää ENISAn neuvoa-antavaa ryhmää ja kansallisten yhteyshenkilöiden verkostoa arvokkaasta palautteesta.
Kiitämme lisäksi ENISAn tilannetietoisuutta ja kyberhäiriöitä koskevia ilmoituksia käsitteleviä ryhmiä niiden aktiivisesta panoksesta ja tuesta erilaisten tietojen kokoamisessa uhkanäkymiin.

OIKEUDELLISET HUOMAUTUKSET

On huomattava, että tämä julkaisu edustaa ENISAn mielipiteitä ja tulkintoja, ellei toisin mainita. Julkaisua ei tule pitää ENISAn tai ENISAn elinten oikeudellisena toimena ilman asetukseen (EU) N:o 2019/881 perustuvaa hyväksyntää. ENISA voi päivittää tätä julkaisua ajoittain.

Kolmannen osapuolen lähteitä lainataan asianmukaisesti. ENISA ei ole vastuussa ulkoisten lähteiden, kuten tässä julkaisussa viitattujen ulkoisen verkkosivujen, sisällöstä.

Tämä julkaisu on tarkoitettu vain tiedoksi. Sen on oltava käytettävissä veloituksetta. ENISA ja sen nimissä toimivat henkilöt eivät ole vastuussa siitä, miten tämän julkaisun sisältämiä tietoja käytetään.

TEKIJÄNOIKEUSILMOITUS

© Euroopan unionin kyberturvallisuusvirasto (ENISA), 2021
Jäljentäminen on sallittua, kunhan lähde mainitaan. Kaikkien sellaisten kuvien tai muun aineiston käyttöön tai jäljentämiseen, joihin ENISAlla ei ole tekijänoikeuksia, on pyydettävä lupa suoraan tekijänoikeuden haltijalta.

ISBN: 978-92-9204-536-4 – DOI: 10.2824/324797 – ISSN: 2363-3050

SISÄLLYSLUETTELO

TIIVISTELMÄ

Tämä on yhdeksäs ENISAn Threat Landscape (ETL) -raportti. Se on vuotuinen raportti kyberturvallisuuden uhkakuvista, ja siinä yksilöidään pääasialliset uhat, uhkiin liittyvät merkittävät suuntaukset, uhkatoimijat ja hyökkäystekniikat sekä kuvataan asiaankuuluvia lieventäviä toimenpiteitä. Olemme kehittäneet jatkuvasti menetelmiämme uhkanäkymien tunnistamiseksi, ja tänä vuonna työtä on tukenut äskettäin perustettu, kyberturvallisuuden uhkanäkymiä käsittelevä tilapäinen työryhmä.

Vuoden 2021 ETL-raportti kattaa ajanjakson huhtikuusta 2020 heinäkuuhun 2021, ja sitä kutsutaan raportissa ’raportointijaksoksi’. Raportointijaksolla havaittuja ensisijaisia uhkia ovat muun muassa seuraavat:

- **Kiristysohjelmat**
- **Haittaohjelmat**
- **Kryptokaappaukset**
- **Sähköpostiin liittyvät uhat**
- **Dataan kohdistuvat uhat**
- **Saatavuuteen ja eheyteen kohdistuvat uhat**
- **Disinformaatio – väärä tieto**
- **Tahattomat uhat**
- **Toimitusketjuihin kohdistuvat hyökkäykset**

Tässä raportissa käsitellään kahdeksaa ensimmäistä kyberturvallisuusuhkien luokkaa. Toimitusketjuihin kohdistuvia uhkia, eli yhdeksättä uhkaluokkaa, analysoitiin yksityiskohtaisesti niiden erityisen näkyvyyden vuoksi ENISAn toimitusketjuja koskevassa Threat Landscape -raportissa [1].

Kaikkia tunnistettuja uhkia, hyökkäystekniikoita, merkittäviä kyberhäiriöitä ja suuntauksia käsitellään yhdessä ehdotettujen lieventävien toimenpiteiden kanssa. Suuntausten suhteen ENISA korostaa raportointijaksolla seuraavaa:

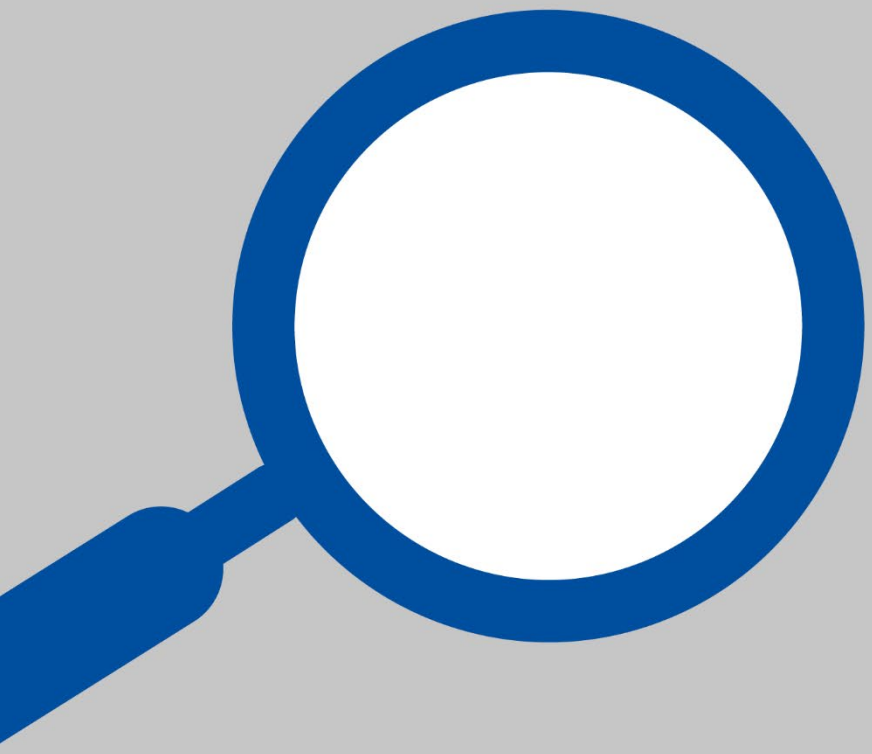
- **Kiristysohjelmat** on arvioitu **suurimmaksi uhkaksi vuosina 2020–2021**.
- **Valtiolliset organisaatiot ovat tehostaneet toimintaansa** sekä kansallisella että kansainvälisellä tasolla.
- **Verkkorikollisia motivoi yhä enemmän toiminnan rahaksi muuntaminen**, esimerkiksi kiristysohjelmilla. **Kryptovaluutta** on edelleen yleisin uhkatoimijoiden maksumenetelmä.
- Vuonna 2020 havaittu **haittaohjelmien väheneminen** jatkuu vuonna 2021. Vuonna 2021 uhkatoimijat turvautuivat yhä useammin verrattain uusiin tai epätavallisiin ohjelmointikieliin koodinsa siirtämiseksi.
- **Kryptokaappausten** määrä oli vuoden 2021 ensimmäisellä neljänneksellä **ennätyksellisen suuri** viime vuosiin verrattuna. Kryptokaappauksiin liittyvä **taloudellinen hyöty** kannusti uhkatoimijoita toteuttamaan hyökkäyksiä.
- **Covid-19 on edelleen suosituin houkuteaihe** sähköpostihyökkäyksiä koskevissa kampanjoissa.
- **Terveydenhuoltoalaan liittyvät tietoturvaloukkaukset lisääntyivät äkillisesti.**
- **Perinteiset hajautetut palvelunestohyökkäyskampanjat** vuonna 2021 ovat kohdennetumpia, sinnikkäämpiä ja monitahoisempia. **Esineiden internet matkaviestinverkkoihin** yhdistettynä johtaa uuteen hajautettuun palvelunestohyökkäysaaltoon.
- Vuosina 2020 ja 2021 havaittiin **piikki tahattomissa kyberhäiriöissä**, sillä covid-19-pandemia aiheutti **inhimillisten virheiden** ja **järjestelmävirheiden** kerrannaisvaikutuksen jopa siinä määrin, että suurin osa vuonna 2020 tapahtuneista tietoturvaloukkauksista johtui virheistä.

[1] ENISAn toimitusketjuja koskeva Threat Landscape -raportti, heinäkuu 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

Uhkatoimijoihin, niiden motivaatioihin ja tavoitteisiin liittyvien suuntausten ymmärtäminen auttaa suuresti kyberturvallisuuspuolustuksen ja lieventämisstrategioiden suunnittelussa. Tämä on olennainen osa yleistä uhka-arviotamme, sillä sen avulla voidaan priorisoida turvallisuuden valvontaa ja laatia erityinen strategia, joka perustuu uhkien toteutumisen mahdolliseen vaikutukseen ja todennäköisyyteen. Tätä taustaa vasten vuoden 2021 ETL:ää sovellettaessa otetaan huomioon seuraavat neljä kyberturvallisuuden uhkatoimijoiden luokkaa:

- **valtion tukemat toimijat**
- **kyberrikollisuuden toimijat**
- **kaupalliset hakkerit**
- **hakkeriaktivistit**

ENISA on jatkuvasti analysoinut kehityssuuntauksia ja merkittäviä seikkoja kustakin vuoden 2021 ETL:ssä esitetystä olennaisesta uhasta. Tämän arvioinnin keskeiset havainnot ja arviot perustuvat useisiin julkisesti saatavilla oleviin resursseihin, jotka esitetään tämän asiakirjan laatimisessa käytetyissä viitteissä. Raportti on suunnattu pääasiassa strategisille ja poliittisille päättäjille, mutta se on hyödyllinen myös tekniselle kyberturvallisuusyhteisölle.



UHKANÄKYMÄN YLEISKATSAUS

Yhdeksännessä ENISAn Threat Landscape -raportissa (ETL) esitetään yleiskuva kyberturvallisuuden uhkanäkymistä. ETL-raportti on osittain strateginen ja osittain tekninen, ja siinä on merkityksellisiä tietoja sekä teknistä tietoa tarvitseville että muille lukijoille. Tämän vuoden työtä on tukenut äskettäin perustettu kyberturvallisuuden uhkanäkymiä käsittelevä tilapäinen työryhmä (CTL)[2].

Kyberturvallisuushyökkäykset ovat lisääntyneet edelleen vuosina 2020 ja 2021 sekä vektorien ja määrän että vaikutusten osalta. Covid-19-pandemia on myös – odotuksien mukaisesti – vaikuttanut kyberturvallisuusuhkaympäristöön. Yksi covid-19-pandemian pitkäkestoisista seurauksista on pysyvä siirtyminen hybridityömalliin. Sen vuoksi pandemiaan liittyvät kyberturvallisuusuhat ja ”uuden normaalin” mukanaan tuomien haavoittuvuuksien hyväksikäyttö ovat yleistymässä. Tämä suuntaus on lisännyt hyökkäyspinta-alaa, minkä seurauksena organisaatioihin ja yrityksiin kotitoimistojen kautta kohdistettujen kyberhyökkäysten määrä on kasvanut[3].

Kyberturvallisuusuhat ovat yleisesti ottaen lisääntymässä. Kyberturvallisuusympäristö on kasvanut hyökkäysten kehittyneisyyden, monimutkaisuuden ja vaikutusten osalta seurauksena siitä, että verkon käyttö lisääntyy jatkuvasti, perinteiset infrastruktuurit siirtyvät verkko- ja pilvipalvelupohjaisiin ratkaisuihin, yhteenliitettävyys kehittyy ja hyödynnetään uusien teknologioiden uusia piirteitä, kuten tekoälyä[4][5]. Erityisesti toimitusketjuihin kohdistuvat uhat ja niiden merkitys, joka johtuu niiden mahdollisesti katastrofaalisista kerrannaisvaikutuksista, ovat saavuttaneet korkean aseman suurimpien uhkien joukossa ja ENISA on luonut tälle uhkatyypille oman uhkaluokan[6].

On syytä huomata, että tässä ETL-raportin iteroinnissa on kiinnitetty erityistä huomiota kyberuhkien vaikutuksiin eri aloilla, myös verkko- ja tietoturvadirektiivissä luetelluilla aloilla. Uhkanäkymien suhteen voidaan saada mielenkiintoista tietoa kunkin alan erityispiirteistä sekä mahdollisista keskinäisistä riippuvuussuhteista ja tärkeistä aihealueista. Alakohtaisiin uhkanäkymiin olisi näin ollen kiinnitettävä enemmän huomiota.

Kyberympäristön turvallisuuden puolesta työskentelevät ja poliittiset päättäjät ovat myös toteuttaneet merkittäviä toimia tänä vuonna. Maailmanlaajuinen yhteisö on alkanut ymmärtää viestinnän ja yhteistyön merkityksen kyberrikollisten tutkinnassa ja jäljittämisessä, ja erityisesti kiristysohjelmista (merkittävin uhka vuoden 2021 ETL-raportin raportointijaksolla) on tullut keskeinen asia globaalien johtajien strategiakokousten esityslistoilla.

Vuoden 2021 ETL-raportin aiempien versioiden lukijat huomaavat, että ensisijaisten uhkien kartoitus on muuttunut. Tänä vuonna ENISA otti askeleen taaksepäin ja yhdisti uhkaluokkia pyrkiessään yhdentämään ja tuomaan paremmin esiin samankaltaisia uhkia. Tämä on osa meneillään olevia toimia uhkaluokitusjärjestelmän uudistamiseksi ja auttaa määrittämään suuntauksia metodologisesti tulevina vuosina.

Vuoden 2021 ETL-raportti perustuu erilaisiin julkisten lähteiden tietoihin ja kyberuhkatiedustelulähteisiin. Siinä yksilöidään tärkeimmät uhat, suuntaukset ja havainnot ja esitetään asiaankuuluvat korkealaatuiset lieventämisstrategiat. ENISA pyrkii parhaillaan vahvistamaan uhkanäkymiä koskevaa raportointimenetelmää työn avoimuuden ja johdonmukaisuuden edistämiseksi.

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – vuoden 2020 raportti tietoturvaloukkausten hinnasta - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] ENISAn tekoälyä koskeva Threat Landscape -raportti: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
[5] https://www.stealthlabs.com/blog/top-10-cybersecurity-trends-in-2021-and-beyond/
[6] ENISAn toimitusketjuihin kohdistuvia hyökkäyksiä koskeva Threat Landscape -raportti, heinäkuu 2021.https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

1.1. ENSISIJAISET UHAT

Vuosien 2020 ja 2021 aikana ilmaantui ja konkretisoitui useita kyberuhkia. Tässä raportissa esitetyn analyysin perusteella ENISAn Threat Landscape -raportissa 2021 yksilöidään seuraavat kahdeksan ensisijaista uhkaryhmää ja keskitytään niihin (ks. Kuvio 1). Näitä kahdeksaa uhkaryhmää korostetaan sen vuoksi, että ne olivat näkyvästi esillä raportointijaksolla, ne olivat yleisiä ja näiden uhkien toteutumisella on ollut merkittäviä vaikutuksia.

- **Kiristysohjelmat**
  Kiristysohjelma on yksi vihamielisen hyökkäyksen tyyppi, jossa hyökkääjät salaavat organisaation tiedot ja vaativat maksua niiden palauttamiseksi. Kiristysohjelmat ovat olleet suurin uhka raportointijaksolla, ja niihin liittyvät tapaukset ovat saaneet paljon näkyvyyttä ja julkisuutta. Kiristysohjelmien uhan merkittävyyttä ja vaikutuksia osoittavat myös useat asiaan liittyvät poliittiset aloitteet Euroopan unionissa (EU) ja koko maailmassa.

- **Haittaohjelmat**
  Haittaohjelma on ohjelmisto tai laiteohjelmisto, jonka tarkoituksena on suorittaa luvaton prosessi, joka vaikuttaa haitallisesti järjestelmän luottamuksellisuuteen, eheyteen tai käytettävyyteen. Haittaohjelmien uhka on usean vuoden ajan ollut tasaisen suuri, vaikka se väheni vuoden 2021 ETL-raportin raportointijaksolla. Uusien liitäntätekniikoiden käyttö ja eräät lainvalvontayhteisön merkittävät saavutukset ovat vaikuttaneet uhkatoimijoiden toimintaan.

- **Kryptokaappaukset**
  Kryptokaappaus tai salainen kryptolouhinta on kyberrikollisuuden tyyppi, jossa rikollinen käyttää salaa uhrin laskentatehoa kryptovaluutan tuottamiseen. Kryptovaluuttojen yleistyessä ja niiden suosion kasvaessa suuren yleisön keskuudessa on havaittu, että vastaavat kyberturvallisuusongelmat ovat lisääntyneet.

- **Sähköpostiin liittyvät uhat**
  Sähköpostiin liittyvät hyökkäykset ovat joukko uhkia, joissa hyödynnetään pikemminkin inhimillisiä ja arkitottumusten heikkouksia kuin tietojärjestelmien teknisiä haavoittuvuuksia. Huolimatta monista tämäntyyppisiin hyökkäyksiin keskittyvistä valistus- ja koulutuskampanjoista uhka pysyy edelleen huomattavana. Erityisesti yritysten sähköpostien vaarantuminen ja rahalliseen hyötymiseen käytettävien kehittyneiden tekniikoiden käyttö on lisääntymässä.

- **Dataan kohdistuvat uhat**
  Tähän luokkaan kuuluvat tietoturvaloukkaukset ja -vuodot. Tietoturvaloukkaus tai tietovuoto tarkoittaa arkaluonteisten, luottamuksellisten tai suojattujen tietojen pääsemistä epäluotettavaan ympäristöön. Tietoturvaloukkaukset voivat johtua kyberhyökkäyksestä, sisäpiiriläisen rikkomuksesta tai tahattomasta tietojen katoamisesta tai paljastumisesta. Uhka on edelleen suuri, sillä tietoihin pääsy on iskujen tekijöiden ensisijainen tavoite useista syistä, esimerkiksi kiristyksen, lunnaiden, kunnianloukkauksen, väärän tiedon levittämisen jne. vuoksi.

- **Saatavuuteen ja eheyteen kohdistuvat uhat**
  Saatavuus ja eheys ovat moninaisten uhkien ja hyökkäysten, esimerkiksi palvelunesto- ja verkkohyökkäysten, kohteena. Koska hajautetut palvelunestohyökkäykset liittyvät läheisesti verkkopohjaisiin hyökkäyksiin, ne ovat yksi kriittisimmistä tietojärjestelmiin kohdistuvista uhista. Ne kohdistuvat järjestelmien käytettävyyteen käyttämällä resursseja loppuun, mikä heikentää suorituskykyä, johtaa tietojen menetykseen ja palvelukatkoksiin. Uhka on jatkuvasti korkealla sijalla ENISAn uhkanäkymissä, koska se ilmenee todellisina tapahtumina ja sen vaikutukset voivat olla laajoja.

- **Disinformaatio – väärä tieto**
  Disinformaatio- ja vääristelykampanjat ovat lisääntymässä, mikä johtuu sosiaalisen median alustojen ja verkkomedian käytön lisääntymisestä sekä ihmisten lisääntyneestä verkossa viettämästä ajasta covid-19-pandemian seurauksena. Nämä uhat on otettu ensi kertaa mukaan ETL-raporttiin, mutta niiden merkitys kyberympäristössä on suuri. Hybridihyökkäyksissä käytetään usein disinformaatio- ja vääristelykampanjoita yleisen luottamuksen heikentämiseksi. Luottamus on merkittävä kyberturvallisuustekijä.

- **Tahattomat uhat**
  Uhkia pidetään yleisesti tahallisina ja haitallisina toimina, joihin osallistuvilla on tiettyjä tarkoitusperiä hyökätä tiettyyn kohteeseen. Tähän ryhmään kuuluvat uhat, joissa pahantahtoinen tarkoitus ei ole ilmeinen. Ne perustuvat pääasiassa inhimillisiin virheisiin ja järjestelmävirheisiin, mutta ne voivat koskea myös fyysisiä ongelmatilanteita, jotka kohdistuvat tietoteknisiin infrastruktuureihin. Nämä uhat ovat luonteeltaan sellaisia, että niitä esiintyy jatkuvasti vuotuisissa uhkanäkymissä, ja ne ovat suuri huolenaihe riskinarvioinnissa.

Kuvio 1: ENISAn Threat Landscape -raportti 2021 – ensisijaiset uhat

On huomattava, että edellä mainittuihin uhkiin sisältyy uhkaluokkia ja yhteen kerättyjä uhkia, jotka on koottu yhteen edellä mainittujen kahdeksan alan alle. Kutakin uhkaryhmää analysoidaan tarkemmin tässä raportissa omassa luvussaan, jossa käsitellään ryhmän erityispiirteitä sekä tarkempia tietoja, havaintoja, suuntauksia, hyökkäystekniikoita ja hillitsemisvektoreita.

1.2. KESKEISET SUUNTAUKSET

Jäljempänä olevassa luettelossa esitetään yhteenveto tärkeimmistä suuntauksista, joita kyberuhkanäkymissä on havaittu raportointijaksolla. Näitä tarkastellaan yksityiskohtaisesti myös ENISAn Threat Landscape 2021 - raportin eri luvuissa.

- **Erittäin pitkälle kehitetyt ja suurivaikutteiset toimitusketjun vaarantumiset** lisääntyivät, kuten ENISAn toimitusketjuihin keskittyvässä Threat Landscape -raportissa korostetaan. **Hallintapalvelujen tarjoajat** ovat arvokkaita kohteita kyberrikollisille.
- **Covid-19-pandemia edisti kybervakoilua** ja loi **mahdollisuuksia kyberrikollisille.**
- **Valtiolliset organisaatiot ovat tehostaneet toimintaansa** sekä kansallisella että kansainvälisellä tasolla. Valtiot ovat lisänneet pyrkimyksiään estää muiden valtioiden tukemia uhkatoimijoita ja ryhtyä oikeustoimiin niitä vastaan.

- **Verkkorikollisia motivoi yhä enemmän toiminnan rahaksi muuntaminen**, esimerkiksi kiristysohjelmilla. **Kryptovaluutta** on edelleen yleisin uhkatoimijoiden maksumenetelmä.
- Kyberrikollisuushyökkäykset **kohdistuvat ja vaikuttavat yhä useammin kriittiseen infrastruktuuriin**.
- Kaksi yleisintä **kiristysohjelmien tartunnanlevittäjää** ovat edelleen **tietojen kalastelu sähköpostitse ja etäpöytäpalveluilla (RDP) tehtävät väsytyshyökkäykset.**
- Keskittyminen **kiristysohjelma palveluna (RaaS) -tyyppisiin liiketoimintamalleihin** on lisääntynyt vuoden 2021 aikana, minkä vuoksi yksittäisten uhkatoimijoiden asianmukainen kohdentaminen on vaikeaa.
- **Kolminkertaisten kiristysohjelmien** esiintyminen lisääntyi voimakkaasti vuoden 2021 aikana.
- Vuonna 2020 havaittu **haittaohjelmien väheneminen** jatkuu vuonna 2021. Vuonna 2021 uhkatoimijat turvautuivat yhä useammin verrattain uusiin tai epätavallisiin ohjelmointikieliin koodinsa siirtämiseksi.
- **Konttiteknologiaympäristöihin kohdennetuista haittaohjelmista** on tullut paljon yleisempiä, ja niihin on kehitetty uusia keinoja, kuten muistista käytettäviä tiedostottomia haittaohjelmia.
- Haittaohjelmien kehittäjät etsivät keinoja tehdä **käänteismallinnuksesta ja dynaamisesta analyysista vaikeampia**.
- **Kryptokaappaustartuntojen** määrä oli vuoden 2021 ensimmäisellä neljänneksellä **ennätyksellisen suuri** verrattuna viime vuosiin. Kryptovaluuttoihin liittyvä **taloudellinen hyöty** kannusti uhkatoimijoita toteuttamaan hyökkäyksiä.
- **Kryptolouhinnan ja kryptokaappaustoiminnan määrä on vuonna 2021 ennätyksellisen suuri**.
- On nähtävissä, että meneillään on **siirtyminen selainpohjaisesta tiedostopohjaiseen kryptokaappaustoimintaan**.
- **Covid-19 on edelleen suosituin houkuteaihe** sähköpostihyökkäyksiä koskevissa kampanjoissa.
- **Yritysten sähköpostien vaarantuminen** on **lisääntynyt**, siihen käytettävät keinot ovat **kehittyneet** ja siitä on tullut entistä **kohdennetumpaa**.
- **Verkkourkinta palveluna (PhaaS)** -liiketoimintamalli on yleistymässä.
- Uhkatoimijat siirsivät huomionsa **rokotetietoihin** dataan ja tietoihin kohdistuvien uhkien suhteen.
- **Terveydenhuoltoalaan liittyvät tietoturvaloukkaukset lisääntyivät äkillisesti.**
- Perinteiset hajautetut palvelunestohyökkäykset ovat siirtymässä **matkaviestinverkkoihin ja esineiden internetiin**.
- **Kiristykseen liittyvät palvelunestohyökkäykset** (RDOS) ovat palvelunestohyökkäysten uusi rintama.
- **Resurssien jakaminen virtuaalisissa ympäristöissä** vahvistaa hajautettuja palvelunestohyökkäyksiä.
- **Hajautetuista palvelunestokampanjoista** on vuonna 2021 tullut kohdennetumpia ja paljon sitkeämpiä ja monitahoisempia.
- **Tekoälyn mahdollistama disinformaatio** tukee hyökkääjien hyökkäyksiä.
- **Verkkourkinta on disinformaatiohyökkäysten ytimessä**, ja siinä hyödynnetään voimakkaasti ihmisten uskomuksia.
- **Väärät tiedot ja disinformaatio** ovat kyberrikollisuuden keskiössä ja lisääntyvät ennennäkemättömällä vauhdilla.
- **Disinformaatio palveluna (DaaS)** -liiketoimintamalli on kasvanut merkittävästi, ja sitä on vauhdittanut covid-19-pandemian kasvava vaikutus ja sen aiheuttama tarve saada enemmän tietoa.
- Vuosina 2020 ja 2021 havaittiin **piikki tahattomissa kyberhäiriöissä**, sillä covid-19-pandemia aiheutti **inhimillisten virheiden** ja **järjestelmävirheiden** kerrannaisvaikutuksia siinä määrin, että suurin osa vuonna 2020 tapahtuneista tietoturvaloukkauksista johtui virheistä.
- **Pilvipalvelujen turvallisuuteen liittyvät tahattomat kyberhäiriöt ovat lisääntyneet**.

1.3. ENSISIJAISTEN UHKIEN LÄHEISYYS EU:HUN NÄHDEN

Tärkeä näkökohta, joka on otettava huomioon ENISAn Threat Landscape -raportin yhteydessä, on kyberuhkien läheisyys suhteessa Euroopan unioniin (EU). Tämä on erityisen tärkeää, jotta voidaan auttaa analyytikoita arvioimaan kyberuhkien merkitystä, korreloimaan ne mahdollisten uhkatoimijoiden ja -vektorien kanssa ja jopa ohjaamaan sopivien kohdennettujen hillitsemisvektorien valintaa. EU:n yhteistä turvallisuus- ja puolustuspolitiikkaa (YTPP)[7] koskevan ehdotetun luokituksen mukaisesti kyberuhat jaotellaan neljään luokkaan, ks. taulukko Taulukko 1.

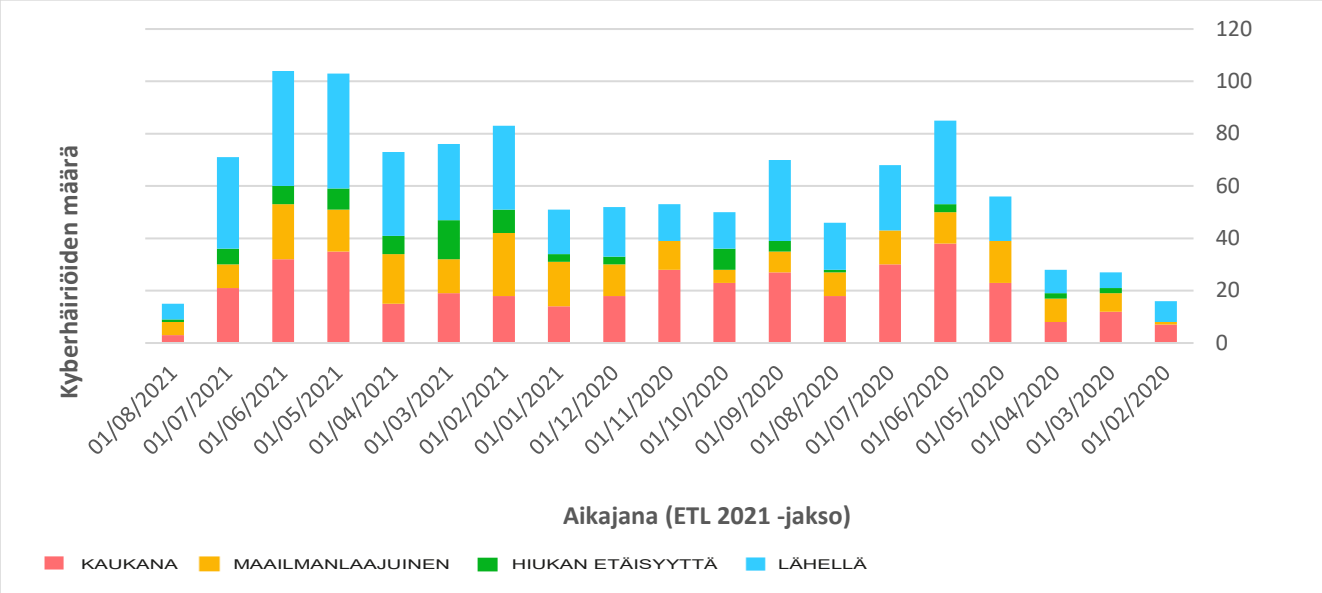
[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

Taulukko 1: Kyberuhkien läheisyyden luokittelu

Läheisyys	Huolenaiheet
LÄHELLÄ	Kohteeksi joutuneet verkot ja järjestelmät, joita valvotaan ja varmennetaan EU:n rajojen sisällä. Kohteeksi joutunut väestö EU:n rajojen sisällä.
HIUKAN ETÄISYYTTÄ	Verkot ja järjestelmät, joita pidetään EU:n digitaalisten sisämarkkinoiden ja verkko- ja tietoturvadirektiivin alaan kuuluvien operatiivisten tavoitteiden kannalta olennaisen tärkeinä, mutta joiden valvonta ja varmuus perustuvat EU:n ulkopuolisiin institutionaalisiin tai jäsenvaltioiden julkisiin tai yksityisiin viranomaisiin. Kohteeksi joutunut väestö EU:n rajojen läheisyydessä sijaitsevilla maantieteellisillä alueilla.
KAUKANA	Verkot ja järjestelmät, joihin kohdistuessaan uhat vaikuttavat ratkaisevasti toiminnallisiin tavoitteisiin EU:n digitaalisilla sisämarkkinoilla ja verkko- ja tietoturvadirektiivin aloilla. Näiden verkkojen ja järjestelmien valvonta ja varmuus hoidetaan EU:n toimielinten tai jäsenvaltioiden julkisten tai yksityisten viranomaisten ulkopuolella. Kohteeksi joutunut väestö kaukana EU:sta sijaitsevilla maantieteellisillä alueilla.
MAAILMANLAAJUINEN	Kaikki edellä mainitut alueet

Kuvio 2 kuvaa vuoden 2021 ETL-raportissa raportoituihin ensisijaisiin uhkaluokkiin liittyvien kyberhäiriöiden aikajanaa. On huomattava, että kuvion tiedot perustuvat julkisiin lähteisiin perustuvan tiedustelun (OSINT) tietoihin ja ovat tulosta ENISAn toiminnasta tilannetietoisuuden alalla[8].

Kuvio 2: Suuriin ETL-uhkiin (OSINT-tietoihin pohjautuva tilannetietoisuus) liittyvien havaittujen kyberhäiriöiden aikajana suhteessa niiden läheisyyteen.



Kuten edellä olevasta kuviosta käy ilmi, vuonna 2021 kyberhäiriöiden määrä on kasvanut vuoteen 2020 verrattuna. Erityisesti LÄHELLÄ-luokassa on jatkuvasti kasvava määrä havaittuja kyberhäiriöitä, jotka liittyvät ensisijaisiin uhkiin, mikä osoittaa niiden merkityksen EU-kontekstissa. Ei ole yllättävää, että kuukausittaiset suuntaukset (jotka eivät näy kuviossa) ovat varsin samanlaisia eri luokituksissa, koska kyberturvallisuus ei tunne rajoja ja koska useimmissa tapauksissa uhkat toteutuvat kaikilla läheisyystasoilla. On huomattava, että vuoden 2021 ETL-raportin kattamien viimeisten kuukausien

[8] Kyberturvallisuusasetuksen 7 artiklan 6 kohdan mukaisesti https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

aikana EU:n LÄHELLÄ-luokan yleisyys on lisääntynyt. ENISA seuraa edelleen tätä suuntausta, sen kehittymistä ja sitä, miten se suhteutuu uhkatoimijoiden ja nykyisten uhkavektorien toimintaan.

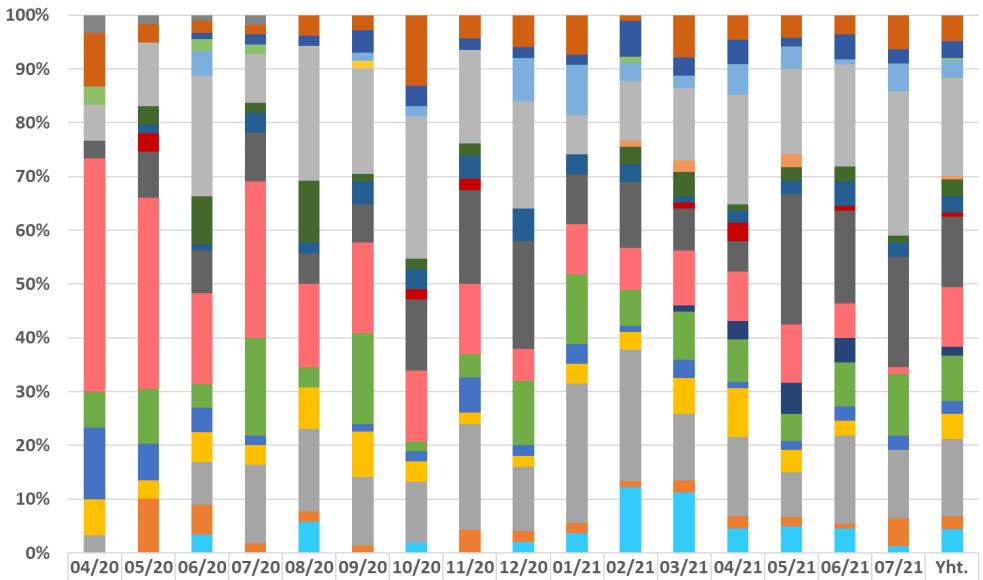
1.4. ENSISIJAISET UHAT ALOITTAIN

Kyberuhat eivät yleensä rajoitu tietylle alalle, ja useimmissa tapauksissa ne vaikuttavat useampaan kuin yhteen alaan. Tämä pitää paikkansa, koska monissa tapauksissa uhat ilmenevät eri aloilla käytettävien taustalla olevien tieto- ja viestintäteknisten järjestelmien haavoittuvuuksien hyödyntämisenä. On kuitenkin otettava huomioon kaikki kohdennetut hyökkäykset sekä hyökkäykset, joissa hyödynnetään kyberturvallisuuden tehokkuuseroja eri aloilla ja tiettyjen alojen suosiota tai näkyvyyttä. Nämä tekijät vaikuttavat uhkiin, jotka ilmenevät kyberhäiriöinä tietyillä aloilla, minkä vuoksi on tärkeää tarkastella havaittujen kyberhäiriöiden ja uhkien alakohtaisia näkökohtia perusteellisesti. Lisäksi kullakin alalla ja eri alojen välisissä riippuvuussuhteissa huomatut suuntaukset ovat havaintoja, jotka voidaan tehdä tällaisen analyysin perusteella.

Kuvioissa 3 ja 4 esitetään alat, joihin vaikutukset kohdistuvat OSINT-tietojen perusteella, ja ne ovat tulosta ENISAn toiminnasta tilannetietoisuuden alalla[9]. Niissä viitataan kyberhäiriöihin, jotka liittyvät vuoden 2021 ETL-raportin ensisijaisiin uhkiin. Tämä on ENISAn ensimmäinen yritys kartoittaa uhkien vaikutuksia tiettyihin aloihin. Tulevina vuosina ja uhkaympäristön tulevissa iteraatioissa pyritään sovittamaan alat yhteen verkko- ja tietoturvadirektiivissä ja sen tarkistamista koskevassa ehdotuksessa (NISD 2.0) lueteltujen alojen kanssa.

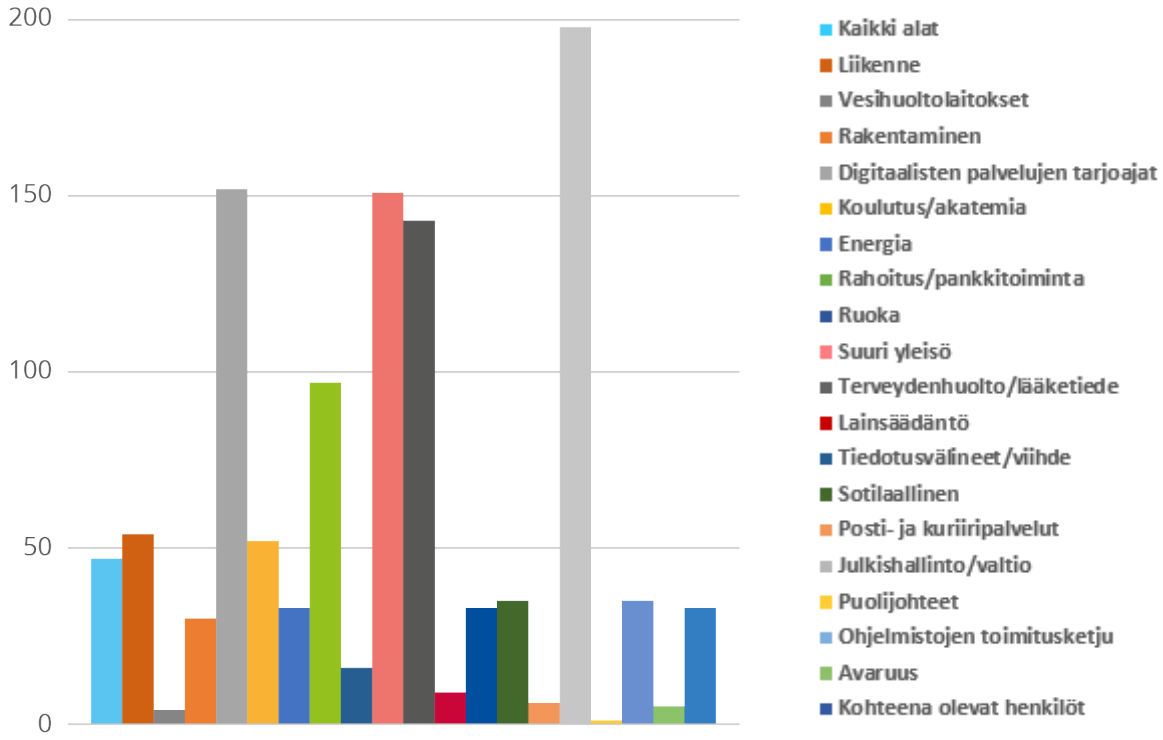
[9]EU:n kyberturvallisuusasetuksen 7 artiklan 6 kohdan mukaisesti (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

Kuvio 3: ETL-raportissa mainittuihin ensisijaisiin uhkiin liittyvien havaittujen kyberhäiriöiden aikajana kohdealan suhteen.



	04/20	05/20	06/20	07/20	08/20	09/20	10/20	11/20	12/20	01/21	02/21	03/21	04/21	05/21	06/21	07/21	Yht.
Vesihuoltolaitokset	1	1	1	1													2
Liikenne	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Kohteena olevat henkilöt			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Avaruus	1		2	1							1						4
Ohjelmistojen toimitusketju			4			1	1		4	5	3	2	5	5	1	4	35
Puolijohteet						1											1
Julkishallinto/valtio	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Posti- ja kuriiripalvelut											1	2		3			6
Sotilaallinen		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Tiedotusvälineet/viihde		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Lainsäädäntö		2					1	1				1	3		1		7
Terveydenhuolto/lääketiede	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Suuri yleisö	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Ruoka												1	3	7	5		16
Rahoitus/pankkitoiminta	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Energia	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Koulutus/akatemia	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Digitaalisten palvelujen tarjoajat	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Rakentaminen		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Kaikki alat			3		3		1		1	2	11	10	4	6	5	1	47

Kuvio 4: Kohdealat kyberhäiriöiden lukumäärän mukaan (huhtikuu 2020 – heinäkuu 2021)



Raportointijakson aikana suuri määrä kyberhäiriöitä kohdistui julkishallintoon, valtiollisten ja digitaalisten palvelujen tarjoajiin. Jälkimmäinen on odotettavissa, kun otetaan huomioon tämän alan palvelujen horisontaalinen tarjonta ja siten sen vaikutus moniin muihin aloihin. Havaittiin myös huomattava määrä kyberhäiriöitä, jotka kohdistuivat loppukäyttäjiin eivätkä välttämättä tietylle alalle. Myös terveydenhuoltoalaan kohdistui merkittäviä häiriöitä, ja tämä toiminta näyttää lisääntyneen raportointijakson viimeisinä kuukausina (touko–heinäkuu 2021). On mielenkiintoista, että rahoitusalalla esiintyy koko vuoden ajan tasainen määrä kyberhäiriöitä. Ohjelmistojen toimitusketjussa näkyy myös kyberhäiriöiden määrän kasvu vuonna 2021. Sama havainto on myös tehty ENISAn toimitusketjuja koskevassa Threat Landscape -raportissa[10].

1.5. MENETELMÄT

ENISAn vuoden 2021 Threat Landscape (ETL) -raportti perustuu avoimista lähteistä saatavilla oleviin tietoihin, jotka ovat pääasiassa luonteeltaan strategisia, ja ENISAn omiin kyberuhkatiedustelutietoihin, ja se kattaa useita aloja, teknologioita ja kontekseja. Raportissa pyritään riippumattomuuteen toimialasta ja toimijoista, ja siinä viitataan eri turvallisuustutkijoiden työhön, turvallisuusblogeihin ja uutisartikkeleihin useissa alaviitteissä. Vuoden 2021 ETL-raportti kattaa ajanjakson huhtikuusta 2020 heinäkuuhun 2021, ja sitä kutsutaan raportissa ’raportointijaksoksi’.

Vuoden 2021 ETL-raportin laatimisessa käytettiin seuraavaa lähestymistapaa. Euroopan unionin kyberturvallisuusvirasto (ENISA) keräsi tilannetietoisuuden keinoin koko kyseessä olevan ajanjakson ajan luetteloa merkittävistä kyberhäiriöistä sellaisina kuin ne ilmenivät avoimissa lähteissä. Tämä luettelo oli perustana ensisijaisten uhkien luettelon määrittämiselle sekä useiden suuntausten ja tilastojen lähdemateriaalina raportissa.

Tämän jälkeen ENISA ja ulkopuoliset asiantuntijat tekivät perusteellisen asiakirjatutkimuksen avoimista lähteistä saatavilla olevasta kirjallisesta materiaalista, kuten uutisartikkeleista, asiantuntijalausunnoista, tiedusteluraporteista, kyberhäiriöiden analysoinnista ja turvallisuustutkimusraporteista. Kyberturvallisuusvirasto on jatkuvasti analysoinut kehityssuuntauksia ja kohdepisteitä kunkin vuoden 2021 ETL-raportissa esitetyn merkittävimmän uhan osalta.

[10] ENISAn toimitusketjuja koskeva Threat Landscape -raportti, heinäkuu 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Tämän arvioinnin keskeiset havainnot ja arviot perustuvat useisiin julkisesti saatavilla oleviin resursseihin, jotka esitetään tämän asiakirjan laatimisessa käytetyissä viitteissä.

Raportissa pyritään erottamaan toisistaan se, mitä lähteet ovat raportoineet, ja mikä on viraston oma arvio. (Käytämme tässä nimenomaisesti ilmaisua ”arvioinnissamme”). Lopuksi arviointia tehdessämme ilmaisemme todennäköisyysarviota esimerkiksi sanoilla todennäköinen, erittäin todennäköinen, varma[11].

MITRE ATT&CK® -kehystä[12] käytettiin tässä raportissa tuomaan esiin tiettyyn uhkaan liittyviä hyökkäystaktiikoita ja -tekniikoita (ks. liite A). Kunkin ATT&CK®-taktiikan osalta esitetään vastapuolen tekniikat. Tämä voi johtaa siihen, että laaditaan luettelo ATT&CK-lieventämistoimenpiteistä[13], joita voidaan soveltaa. MITRE ATT&CK® on tietopohja, joka tarjoaa yhteisen määritelmän vastapuolen taktiikoille ja tekniikoille, jotka perustuvat todellisissa asiayhteyksissä tehtyihin havaintoihin. MITRE ATT&CK® -tietopohjaa käytetään perustana erityisten uhkamallien ja -menetelmien kehittämiselle yksityisellä sektorilla, valtionhallinnossa sekä kyberturvallisuustuote- ja palveluyhteisössä.

Raportin vahvisti ENISAn huhtikuussa 2021 perustettu kyberuhkanäkymiä käsittelevä tilapäinen työryhmä[14], joka koostuu eurooppalaisten ja kansainvälisten julkisen ja yksityisen sektorin toimijoiden asiantuntijoista.

Threat Landscape -raportin tulevaa kehittämistä varten ENISA on parhaillaan virallistamassa uutta menetelmää, jolla edistetään avoimuutta ja luodaan perusta jäsennellyille ja hyvin sovitetuille prosesseille. Tämän pyrkimyksen tavoitteena on tulevaisuudessa julkistaa uhkanäkymiä koskevat menetelmät yhdessä tarkistetun uhkaluokitusjärjestelmän kanssa.

1.6. RAPORTIN RAKENNE

ENISAn vuoden 2021 Threat Landscape (ETL) -raportti on säilyttänyt aiempien ETL-raporttien rakenteen käyttämällä samanlaista rakennetta korostamaan tärkeimpiä kyberuhkia vuonna 2021. Aiempien iteraatioiden lukijat voivat huomata, että uhkaluokkia on yhdistetty uutta kyberturvallisuusuhkien luokitusjärjestelmää varten, jota on tarkoitus käyttää tulevaisuudessa.

Raportin rakenne on seuraava:

Luvussa 2 tarkastellaan uhkatoimijoihin liittyviä suuntauksia (esim. valtion tukemat toimijat, kyberrikollisuuden toimijat, kaupalliset hakkerit ja hakkeriaktivistit).
Luvussa 3 käsitellään kiristysohjelmia koskevia tärkeimpiä havaintoja, kyberhäiriöitä ja suuntauksia.
Luvussa 4 esitellään haittaohjelmia koskevat tärkeimmät havainnot, kyberhäiriöt ja suuntaukset.
Luvussa 5 kuvataan kryptokaappauksiin liittyviä tärkeimpiä havaintoja, kyberhäiriöitä ja suuntauksia.
Luvussa 6 esitellään sähköpostiin liittyviä uhkia koskevia keskeisiä havaintoja, kyberhäiriöitä ja suuntauksia.
Luvussa 7 käsitellään dataan kohdistuvia uhkia koskevia tärkeimpiä havaintoja, kyberhäiriöitä ja suuntauksia.
Luvussa 8 esitellään saatavuuteen ja eheyteen kohdistuvia uhkia koskevat tärkeimmät havainnot, kyberhäiriöt ja suuntaukset.
Luvussa 9 korostetaan hybridiuhkien merkitystä ja kuvataan disinformaatiota ja väärää tietoa koskevia keskeisiä havaintoja, kyberhäiriöitä ja suuntauksia.
Luvussa 10 keskitytään tahattomiin uhkiin liittyviin merkittäviin havaintoihin, kyberhäiriöihin ja suuntauksiin.
Liitteessä A esitetään kunkin uhan osalta yleisesti käytetyt tekniikat, jotka perustuvat MITRE ATT&CK® -kehykseen.
Liite B sisältää raportointijakson aikana havaitut merkittävät kyberhäiriöt uhkaa kohden.

[11] CIA - todennäköisyyden arvioinnissa käytetyt sanat https://www.cia.gov/static/0aae8f84700a256abf63f7aad73b0a7d/Words-of-Estimative-Probability.pdf
[12] MITRE ATT&CK® , https://attack.mitre.org/
[13] https://attack.mitre.org/mitigations/enterprise /
[14] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes