Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025

Euroopan unionin osarahoittama

XAMK
Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Euroopan unionin osarahoittama

Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025

Sisällys

Euroopan unionin osarahoittama

Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025

Johdanto

Digitalisaation murros voidaan nähdä alkaneeksi jo 1970-luvulla, ja siitä asti rikolliset ovat omaksuneet digitalisaation tuomat mahdollisuudet omaan liiketoimintaansa. Käsite **Crime-as-a-Service (CaaS)** viittaa rikollisten liiketoimintamalleihin, joissa nämä tarjoavat erilaisia palveluja ja työkaluja toisille rikollisille rahallista korvausta vastaan. Tällaiset palvelut voivat kattaa laajan valikoiman rikollisia toimintoja, kuten tietomurtoja, identiteettivarkauksia, ihmis- sekä huumekauppaa, kyberhyökkäyksiä ja paljon muuta. **CaaS-ilmiö** ja erityisesti **Cybercrime-as-a-Service -malli** on noussut esiin digitaalisen aikakauden myötä, ja se on synnyttänyt huolta digitaalisen rikollisuuden laajenemisesta ja monipuolistumisesta myös Kymenlaaksossa. Vaikka Suomi onkin yleisesti ottaen turvallinen maa, erityisesti ulkopuolelta tuleva digitaalinen rikollisuus on alati kasvava uhka, joka voi vaikuttaa negatiivisesti alueen asukkaisiin ja yrityksiin.

Yksi Cybercrime-as-a-Service-ilmiön huolestuttavimmista piirteistä on rikollisten työkalujen ja palveluiden helppo saatavuus. Tämä madaltaa kynnystä perinteisesti monimutkaisille rikoksille, kuten tietomurroille ja haittaohjelmien levittämiselle, tehden niistä entistä tavallisempia. CaaS tarjoaa välineitä myös henkilöille, joilla ei ole syvällistä teknistä osaamista, mikä lisää rikosten määrää entisestään.

Vaikka Crime-as-a-Service -termi pitää sisällään useita eri ilmiöitä, tullaan selvityksessä erityisesti keskittymään CaaS-ilmiön digitaaliseen puoleen (Cybercrime-as-a-Service) ja sen mahdollisiin alalajeihin, kuten **Ransomware-as-a-Service (RaaS)**, **Malware-as-a-Service (MaaS)** jne.

Selvityksellä pyritään täyttämään seuraavat tavoitteet:

- **Kyberrikollisuuden käsitteiden avaaminen mahdollisimman helposti ymmärrettävään muotoon.**
- **Tuoda esille uusia näkökulmia kyberrikollisuudesta ja sen järjestäytynyt luonne.**
- **Pyrkiä selvittää CaaS-ilmiön yleistyminen maailmalla ja Suomessa. Tuloksien pohjalta voidaan tehdä johtopäätöksiä Kymenlaakson tilanteeseen.**
- **Tuoda yrityksille esille esimerkkejä ja asiantuntijoiden lausuntoja kyberaseiden ja haittaohjelmien kaupallistamisen vaaroista.**

Selvitys on tehty osana Kyberturvan tulevaisuus Kymenlaaksossa -hanketta, jota rahoitetaan Kymenlaakson liiton kautta Euroopan Unionin Oikeudenmukaisen siirtymän rahastosta (JTF). Hanke toimii Kaakkois-Suomen ammattikorkeakoulun (Xamk) alaisuudessa. Selvityksen vastuuhenkilönä sekä tekijänä toimii kyber- ja tietoturva-asiantuntija Markus Hölsä.

2. Toteutus

Pääaineisto on kerätty asiantuntijoiden teemahaastatteluiden avulla, jotka on anonymisoitu henkilön yksityisyyden turvaamiseksi. Jokaisesta haastateltavasta on tehty henkilöprofiili, joka avaa haastateltavan asiantuntijuutta aiheeseen liittyen. Aihetta tutkitaan asiantuntijahaastatteluiden lisäksi laajalla määrällä kirjallista aineistoa sekä asiantuntijatapahtumista kerättyjen tietojen avulla.

Haastattelut

Teemahaastattelun kysymykset ovat seuranneet yhtenevää kysymysrunkoa, mutta haastattelun aikana on suosittu vapaata ja avointa keskustelua haastattelijan ja haastateltavan välillä. Syy tähän on mahdollisimman runsas tiedonkeruu, joka haastavan aiheen takia on oleellista oikeiden johtopäätösten tekemiseen ja selvitystavoitteiden täyttämiseen.

Asiantuntija 1:

Henkilö on toiminut aikaisemmin tiiminvetäjänä kyber- ja teknologiadiplomatiassa ja auttanut vastaamaan siihen liittyvissä kysymyksissä. Aiemmin hän on työskennellyt tutkimuslaitoksessa projektitutkijana ja korkeakoulussa väitöskirjatutkijana.

Uudessa roolissaan hän vastaa kyberturvallisuushankkeiden seurannasta ja raportoinnista sekä osallistuu eri valtionhallinnon kyberturvallisuushankkeisiin. Lisäksi hänen tehtävänään on koordinoida ja sovittaa yhteen kansallista kyberturvallisuuden kehittämistä, suunnittelua ja varautumista osana toimin-taympäristön muutoksia.

Asiantuntija 2:

Henkilö työskentelee aktiivisesti poliisin kanssa tehden ennalta estävää erityistoimintaa, jolla estetään vakavaa tietoverkkorikollisuutta ja siitä aiheutuvaa inhimillistä kärsimystä ja vahinkoa yksilön, organisaatioiden ja yhteiskunnan näkökulmasta. Henkilö on tehnyt ennaltaehkäisevää työtä verkkorikollisten parissa ja sitä kautta saanut kattavan kuvan rikolliseen toimintaan.

Asiantuntija 3:

Henkilö toimii etulinjassa Suomeen kohdistettuja kyberhyökkäyksiä vastaan. Hänen työhönsä kuuluu kyberturvatilannetta koskevien raporttien laatiminen yrityksille ja organisaatioille sekä aktiivisen kybertilannekuvan luominen Suomen väestölle. Henkilön työ kyberrikollisuutta vastaan on antanut hänelle yksityiskohtaista tietoa rikollisten toiminnasta ja sen tehokkuudesta.

Asiantuntija 4:

Henkilöllä on yli 20 vuoden työkokemus kyberturvallisuudesta. Hänen erikoisalanansa on tietomurtojen selvittäminen sekä kyberkriisien hallinta. Henkilö on tutkinut useita tietomurtoja sekä kiristyshaittaohjelmaryhmien toimintaa. Henkilö tuntee ryhmien toimintatavat ja osaa avata niiden toimien vakavuutta yrityksiin ja organisaatioihin.

Asiantuntija 5:

Henkilöllä on kattava osaaminen tietoturvahallintakeskuksen (SOC) toiminnasta Suomen yrityskentällä. SOC-toiminnan tehostamiseksi henkilö on ollut aktiivisesti mukana tutkimassa pimeän verkon kauppapaikkojen datan myyntiä. Sitä kautta hän on kerännyt arvokasta tietoa tulevista hyökkäyksistä.

Euroopan unionin osarahoittama

Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025

3. Rikos ja sen kaupallistaminen

Rikollisuuden palvelumalli on vaikeaa määrittää täsmällisesti, koska rikollisuuden lajeja on niin paljon. Rikollisuutta on tarjottu palveluna kautta historian moniin eri tarkoituksiin, esimerkiksi kylmän sodan aikana valtiolliset toimijat ostivat rikollisia palveluita omien operaatioidensa toteuttamisessa. Internetin yleistymisen myötä rikolliset palvelut ovat yleistyneet ja yhä useamman on mahdollista ostaa niitä globaalilta kauppapaikalta. Verkon välityksellä rikolliset tarjoavat hyvinkin kattavia rikosinfrastruktuureja muille rikollisille.

Keskeisiä Cybercrime-as-a-Service -toimintamalleja ovat:

- **Ransomware-as-a-Service (RaaS):** **Ransomware, eli lunnashaittaohjelmien vuokraaminen, joissa hyökkääjät saavat valmiit työkalut kiristysohjelmien käyttöön ja jakoon. Lunnashaittaohjelma on rikollisten ja valtiollisten tahojen käyttämä haitallinen ohjelmisto, jonka tavoitteena on salata laite ja estää sen käyttö. Salauksesta pääsee usein eroon vain maksamalla pyydetty lunnasvaatimus.**
- **Botnet-rentals:** **Bottiverkkojen käyttö, joita voidaan vuokrata massiivisten hyökkäysten suorittamiseen.**
- **Phishing-kampanjoiden myynti:** **Phishing-tekniikoiden ja työkalujen vuokraaminen tai ostaminen helpottaa identiteettivarkauksien ja tietomurtojen toteuttamista.**
- **Malware-as-a-Service (MaaS):** **Haittaohjelmia rakentavat verkkorikolliset myyvät toisille rikollisille haittaohjelmapaketteja, joita voidaan käyttää muun muassa virusten levittämiseen ja troijalaishyökkäysten suunnitteluun. MaaS-omistajat tarjoavat pääsyn alustalle jäsenmaksua vastaan. Asiakkaat käynnistävät sitten haittaohjelmakampanjansa alustan avulla. (Chebac, A. 2023.)**
- **Vulnerability-discovery-as-a-service:** **Eli VDaaS on CaaS:n alaluokka, jossa pimeässä verkossa toimivat jälleenmyyjät tarjoavat verkko-hyökkäysammattilaisten tai automatisoitujen työkalujen palveluja, joiden avulla he etsivät ja arvioivat tietoturva-aukkoja kohteiden laitteissa, verkoissa tai sovelluksissa. (Slavin, B. 2024.)**
- **Initial access brokers (IAB):** **Ovat rikollisia, jotka myyvät sisäänpääsyä yritysten tai organisaatioiden verkkoinfrastruktuuriin. IAB ovat tärkeitä useille eri kyberrikollisuusryhmille, koska eri päämääristä huolimatta aloitus on kaikille aina sama: hanki pääsy kohdeverkkoon ja ylläpidä pääsyä mahdollisimman pitkään. IAB-palvelu tarjoaa tämän pääsyn.**
- **Crypter & Loader Services:** **Crypter-terminä tarkoittaa työkaluja, tekniikoita ja metodeja, joiden avulla rikolliset tai eri toimijat voivat salata, peittää tai muulla tavoin muuttaa haitallista koodia havaitsemistekniikoiden kiertämiseksi. Loader on haittaohjelma, jota usein käytetään Crypter-toiminnassa toimittamaan lisähyötykuormia, kuten esimerkiksi kryptolouhijoita tai lunnashaittaohjelmia. Crypter- ja Loader-palvelut ovat olennainen osa IAB-verkkorikosekosysteemiä (Matt, S. C. 2024.)**

Euroopan unionin osarahoittama

XAMK
Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Euroopan unionin osarahoittama

Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025

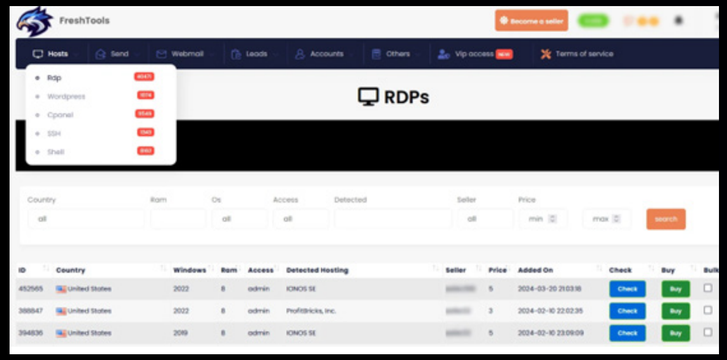
Palveluita on moneen eri lähtöön, ja ne antavat kyberrikollisille tehokkaat työkalut aloittaa laajojakin hyökkäyskampanjoita. Asiantuntija 1 mukaan CaaS-ilmiö on nousujohteinen trendi rikollisten keskuudessa. Sen vuoksi esimerkiksi huijausten ja kiristyshaittaohjelmakampanjoiden määrä on noussut merkittävästi.

Kuten normaalissa yritystoiminnassa, myös rikolliset käyttävät alihankkijoita omien palveluidensa tuottamiseen. Yksi suurimmista kiristyshaittaohjelma ryhmistä nimeltään Akira käyttää asiantuntija 4 mukaan alihankkijapalveluita, esimerkiksi Inital-access (IA) tai vulnerability-discovery operaatioissaan. Samaan tapaan rikollisryhmät voivat myös käyttää erilaisia pimeänverkon kauppapaikkoja käyttäjätunnusten sekä salasanojen ostoon. Pimeän verkon kauppapaikat välittävät rikollisten palveluita hyvin samaan tapaan kuin normaalit julkiverkon kauppapaikat. Asiantuntija 5 mukaan osaan pimeän verkon kauppapaikkaan tai keskustelufoorumiin on usein hyvin vaikea päästä sisään:

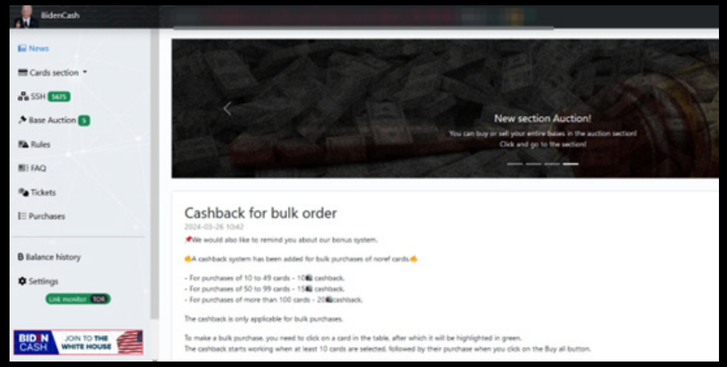
”On myös paljon sellaisia foorumeita, mihin ei lainkuuliaisilta kansalaisilta ole paljon asiaa mennä. Eli pitää esimerkiksi jakaa joko omaa haittaohjelmaa tai jotain varastettua dataa, että hyväksytään jonkun yhteisön jäseneksi”.

Useat pimeän verkon kauppapaikat ovat myös implementoineet keinon myyjien arvosteluun. Asiakas pystyy esimerkiksi antamaan tähtiä palvelun laadusta, tuotteesta tai hinnasta. Tämän avulla kauppapaikoissa luodaan luottamusta asiakkaiden ja rikollisten välillä.

Yllä olevat kuvakaappaukset on otettu kahdesta eri pimeän verkon kauppapaikasta, jotka erikoistuvat erilaisten tunnusten myymiseen.



Kuva 1. Pimeän verkon kauppapaikka FreshTools (SOCRadar. 2024)



Kuva 2. Pimeän verkon kauppapaikka BidenCash (SOCRadar. 2024)

Verkkorikolliset voivat ostaa tämänkaltaisista palveluista itselleen mahdollisen pääsyn yrityksen järjestelmiin. Yritysten tietokannoista varastetuista tietopaketeista voi pyytää suuriakin summia pimeillä kauppapaikoilla, ja todennäköisesti joku on myös valmis maksamaan näistä tiedoista.

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Euroopan unionin osarahoittama

Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025

Category	Product	2020	2021
Credit Card and Banking	Cloned Mastercard with PIN	$15	$25
	Cloned American Express with PIN	$35	$35
	Cloned VISA with PIN	$25	$25
	Credit card details, account balance up to $1000	$12	$150
	Credit card details, account balance up to $5000	$20	$240
	Stolen online banking logins, minimum $100 on account	$35	$40
	Stolen online banking logins, minimum $2000 on account	$65	$120
	Walmart account with credit card attached	$10	$14
Payment Processing Services	Stolen PayPal account details, minimum $100	$199	$30
	PayPal transfer from stolen account, $1000 – $3000	$320	$340
	PayPal transfers from stolen account, $3000+	$156	$180
	Western Union transfer from stolen account, above $1000	$98	$45
Social Media	Hacked Facebook account	$75	$65
	Hacked Instagram account	$55	$45
	Hacked Twitter account	$49	$35
	Hacked Gmail account	$156	$80

Kuva 3. **Pimeän verkon kauppapaikkojen myyntihintoja (Sen, R. 2021)**

Email Database Dumps	Avg. Price USD (2023)
10 million USA email addresses	$120
100 million USA email addresses	$200
5 million UK email addresses	$110
1.2 million USA dentist email addresses	$200
600k New Zealand emails	$110
2.4 million Canada emails	$100

Kuva 4. **Pimeässä verkossa myytävien sähköpostien hintoja (Zoltan, M. 2023)**

Vieressä oleva data tuo esille useita mielenkiintoisia yksityiskohtia varsinkin varastettujen tietojen hinnoittelusta. Esimerkiksi luotto- ja pankkikorttien hinnoittelu avaa ikkunaa kauppapaikkojen ekonomiaan:

- Kloonatut Mastercard, American Express ja VISA-kortit (PIN-koodilla): Nämä ovat kloonattuja maksukortteja, jotka on luotu alkupe-räisen kortin tiedoilla. Hinnat yksittäisille korteille pyörivät 25 $ - 35 $ (24 € - 33 €) hintaluokassa. Kloonattujen korttien toiminta on usein epävarmaa, jonka takia kortteja usein ostetaan tukkuna suuria määriä. Tämä tukkuostaminen alentaa korttien hintaa.
- Luottokorttitiedot ja verkkopankkitunnukset: Jos myyjällä on tietoa luotto- tai pankkitunnusten sisäisistä rahamääristä, voidaan niitä myydä saldon mukaan. Miksi sitten myyjä myy esimerkiksi 2000 $ arvoista pankkitiliä vain 120 $ (114 €) hintaan? Rahojen saaminen pankkiteiltä on yllättävän vaikea prosessi, joka vaatii toimivan rahanpesujärjestelmän. Usein luotto- ja pankkitilien Inital-Access-Brokerit eivät omaa tämänkaltaista osaamista, jonka takia he vain myyvät tunnukset eteenpäin. Samalla he myös piilottavat omia jälkiään ja pienentävät kiinnijäämisen riskiä.

Vieressä kuvatut hinnat eri maiden sähköpostiosoitteille osoittavat, että kaikki ihmiset ovat kiinnostavia ja jossain määrin rahanarvoisia. Tämä kannattaa pitää vahvasti mielessä esimerkiksi sosiaalisessa mediassa, missä on turhan helppo jakaa itsestään liikaa tietoa.

Asiakaskunta

Ketkä sitten ovat niitä, jotka ostavat ja käyttävät CaaS-palveluita? Asiantuntijan 2 mukaan Euroopassa nuorten verkkorikollisuus on ollut nousussa, ja yhä useampi käyttää kybertyökaluja ja ohjelmistoja omissa toimissaan.

”Yleensä siinä varhaisessa vaiheessa puhutaan vielä tämmöisistä lievistä rikoksista, että sitä rajaa koetellaan. Se ei vielä ole taloudellisesti motivoituneita ne rikokset, että yleensä silloin on tämmöistä kokeilunhalua, jonkun jäynän tekemistä tai ihan puhdasta uteliaisuutta”.

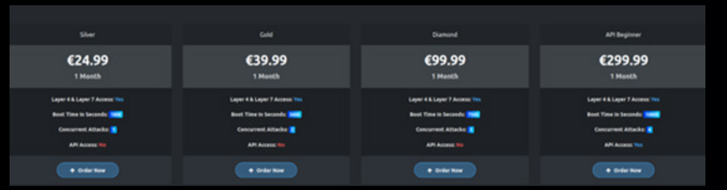
Alla oleva taulukko kuvaa Euroopassa suoritetun kyselyntuloksia. Kyselyllä pyrittiin selvittämään tietoverkkorikollisuuden ja tietoverkkohäirinnän yleistyvyydestä nuorten keskuudessa. Palveluiden oston laajuudesta kertoo tulos, jonka mukaan joka viides nuori on ostanut laittomia tuotteita pimeän verkon kauppapaikoilta.

69,1 prosenttia (N=5507) ilmoittaa syyllistyneensä vähintään yhteen tietoverkkorikollisuuden tai tietoverkkohäirinnän (mahdollisesti riskialtista tai haitallista käyttäytymistä) muotoon (20 keskeisen käyttäytymistavan osalta) viime vuoden aikana.

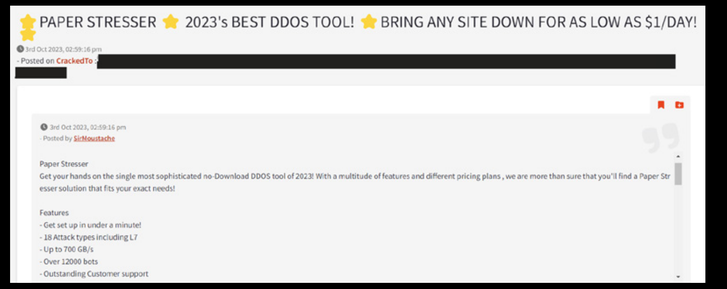
Teko	Yleisyys
Digitaalinen piratismi	Yksi kolmesta
Käyttänyt laittomia virtuaalisia markkinapaikkoja	Yksi viidestä
Rahan salakuljetus (tai rahanpesu)	Yksi kahdeksasta
Verkkohäirintä	Yksi kahdeksasta
Vihapuhe	Yksi kymmenestä
Hakkerointi	Yksi kymmenestä
Verkkokiusaaminen	Yksi kymmenestä
Kalastelu (phishing)	Yksi yhdestätoista
Kostoporno	Yksi yhdestätoista
Verkkopetokset	Yksi yhdestätoista
Identiteettivarkaus	Yksi yhdestätoista
Rasistinen / muukalaisvihamielinen puhe	Yksi yhdestätoista
Sextortion	Yksi kolmestatoista

Kuva 5. Kyselytulokset nuorien tekemistä verkkorikoksista tai tietoverkkohäirinnästä (Davidson ym. 2023)

Verkkorikollisuuden yhteydessä käytetään usein termiä ”Script-kiddies”. Sillä tarkoitetaan yleensä nuorta ja kypsymätöntä hakkeria, joka käyttää valmiita työkaluja ilman todellista teknistä ymmärrystä siitä, mitä ne oikeastaan tekevät tai kuinka ne toimivat. WithSecure on julkaissut aiheesta tutkimuksen, jossa kerrotaan, että tämänkaltaiset osaamattomat, työkaluilla leikkivät script-kiddies (suomeksi skriptipennut) ovat historiaa. Tilalle ovat tulleet nuoret ja nuoret aikuiset, jotka pystyvät luomaan vaikeitakin hyökkäyksiä CaaS:in mahdollistamien resurssien, työkalujen ja oppaiden avulla. (WithSecure whitepaper, 13)



Kuva 6. Pimeän verkon kauppapaikka palvelunestohyökkäyksille (SearchlightCyber. 2023)



Kuva 7. Pimeän verkon kauppapaikka palvelunestohyökkäyksille (SearchlightCyber. 2023)

Euroopan unionin osarahoittama

Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025

Euroopan unionin osarahoittama

Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025

DDOS Attacks	Unprotected website, 10-50k requests per second, 1 month	$750
	Unprotected website, 10-50k requests per second, 1 week	$350
	Europe, low-quality, slow speed, low success rate per 1, 000 requests	$200
	Premium protected website, 20-50k requests per second, multiple elite proxies, 24 hours	$170
	Unprotected website, 10-50k requests per second, 24 hours	$35
	Unprotected website, 10-50k requests per second, 1 hour	$10

Kuva 8. Pimeässä verkossa myytävien palvelunestohyökkäysten myyntihintoja (Zoltan, M. 2023)

Palvelunestoihin valjastetun bottiverkon vuokraaminen ei ole mikään erityisen kallis hankinta. Palvelunestojen halvat hinnat herättävät huolta varsinkin kunnissa ja yrityksissä, missä tahalliseen häirintään ei ole varauduttu. Kyberrikostorjuntakeskuksen päällikkö Mikko Rauhamaa sitaatti Ylen artikkelissa vahvistaa tätä huolta varsinkin silloin, kun toimijana on alaikäinen:

”Pelimaailmassa turhautunut lapsi tai nuori voi haluta estää muiden pelit, jos ei ole tullut haluttua lopputulosta. Tai jos on tulossa Wilma-viestiä, ja ei haluta että vanhemmat näkee, niin koitetaan kaataa Wilma palvelunestohyökkäyksellä.”
(Tillaeus, J. 2023) Yrittäjälle tämänkaltainen palvelu voi muodostua aidoksi riskiksi, jos esimerkiksi huolena on vihastunut asiakas tai mahdollinen kilpailija.

Toinen asiakaskunta, joka hyötyy valmiista rikollispalveluista, on haktivistit. He ovat hakkereita, jotka käyttävät hakkerointia edistääkseen omia ideologioitaan. Venäjän hyökkäyssota ja Israelin sekä Iranin välinen konflikti ovat tehneet haktivismista nykypäivänä paljon yleisempää. Tämänkaltaiset toimijat eivät usein pysty suorittamaan vaativia verkkorikoksia ja turvautuvat siksi pimeän verkon kauppapaikkoihin etsiäkseen haittaohjelmia, tunnuksia tai muita hakkerointityökaluja. Nämä palvelut mahdollistavat

Product	Avg. Price USD (2022)	Avg. Price USD (2023)
Premium-quality, per 1.000	$5.500	$4.500
USA only, medium-quality, 70% success rate, per 1.000 installs	$900	$700
Android OS per 1.000 installs	$950	$650
Europe fresh, high-quality per 1.000 installs	$1.800	$1.600
UK high-quality per 1.000 installs	$1.800	$1.600
USA high-quality, per 1.000 installs	$1.700	$1.500
Europe, medium-quality, 70% success rate, per 1.000 installs	$450	$250
USA, CA, UK, AU med quality, 70% success rate per 1.000 installs	$1.200	$1.100
CA high-quality, per 1.000 installs	$1.200	$1.100
USA, CA, UK, AU low quality, slow speed, low success rate x 1000 installs	$800	$700
Europe, aged, high-quality, per 1.000 installs	$1.100	$1.000
Global, medium-quality, 70% success rate, per 1.000	$115	$75
Global, low quality, slow-speed, low success rate, per 1.000 installs	$45	$35
Europe low-quality, slow-speed, low success rate, per 1.000 installs	$120	$110

Kuva 9. Pimeässä verkossa myytävien haittaohjelmien myyntihintoja (Zoltan, M. 2023)

hyökkäykset yrityksiä ja organisaatioita kohtaan.

Myös haittaohjelmien ostaminen on mahdollista. Tätä ilmiötä kutsutaan nimellä Malware-as-a-Service (MaaS), eli haittaohjelma palveluna. Vardham Rajin (2024) artikkelin mukaan maailmanlaajuisesti päivässä luodaan lähes 300,000 uutta haittaohjelmaa, joista suurimman osan voidaan olettaa menevän myyntiin muille rikollisille.

4. Rakenne

Verkkorikollisuuden tuomat suuret voitot ja kansainväliset markkinat ovat saaneet tietoverkkorikollisryhmät kehittymään ammattimaisemmiksi. Tämä ammattimaisuus näkyy myös rikollisorganisaatioiden kansainvälisissä toimissa sekä niiden kyvyssä pysyä toiminnassa häiriöistä riippumatta. Tämä on mahdollista, koska verkkorikollisorganisaatiot ovat yleensä hyvin modulaarisia ja verkottuneita. Ne koostuvat monista itsenäisistä toimijoista, jotka tekevät yhteistyötä löyhän rakenteen puitteissa. Modulaarisuus tarkoittaa tässä yhteydessä sitä, että eri osa-alueita voidaan ulkoistaa ja ostaa muilta toimijoilta, jolloin organisaatio olisi joustava ja dynaaminen. Dynaamiselle rakenteelle on useita syitä:

- **Identiteetin salaaminen:** Tietoverkkorikollisuus vahvuutena toimii sen maailmanlaajuisuus ja hajautuneisuus. Hajautuneisuuden ansiosta viestintä ja toiminta on helpompi pitää mahdollisimman anonyyminä, koska rikolliset eivät itsekään tunne toisiaan. Hyvin usein rikollisryhmät käyttävät anonyymejä kanavia, kuten Dark Web -foorumeita, salattuja viestintävälineitä sekä kryptovaluuttoja maksamiseen. Anonymiteetti ja hajauttaminen vaikeuttavat rikollisryhmien jäljittämistä. Rikollisryhmät voivat toimia myös kansainvälisesti ilman, että eri maiden viranomaiset voivat helposti valvoa tai estää niiden toimintaa.
- **Yhteistyö ja liittoutumat:** Verkkorikollisryhmät tarvitsevat myös osaavia työntekijöitä omiin operaatioihinsa. Hajautuneisuuden ja anonymiteetin avulla yksittäiset verkkorikolliset voivat olla osallisia useissa eri ryhmissä. Ryhmät myyvät palveluja myös muille ryhmille sekä tarvittaessa ottavat toisen ryhmän jäseniä omaan tiimiinsä, mikäli alkuperäinen ryhmä hajoaa syystä tai toisesta (Fazzini, K. 2019.)
- **Riskin hajauttaminen:** Verkkorikollisten suurimmat uhat tulevat viranomaistahojen toimenpiteistä. Vaikkakin ryhmien toiminta on usein hajaantunutta ja kansainvälistä, eivät nämä toimenpiteet yksinään tuo ryhmille täyttä turvaa. Jakamalla ryhmät pienempiin osastoihin voidaan vähentää riskiä koko operaation hajoamiselle, jos joku jää kiinni.

Verkkorikollisorganisaatiot ovat myös omaksuneet työnjakoon, erikoistumiseen ja hierarkiaan perustuvia liiketoimintamalleja. Tämä helpottaa useiden eri liikkuvien osien hallitsemista. Perinteiseen yritysrakenteeseen perustavia osastoja voi olla esimerkiksi:

- **Henkilöstön rekrytointi ja -hallinta osasto (HR):** Usein rikollisryhmät noudattavat modulaarista ja verkostomaista toimintatapaa. Tämä vähentää riskejä kiinnijäämiselle ja helpottaa alihankintaketjujen hallitsemista sekä myös niiden erottamista. Kuitenkin rikollisryhmät ovat joissakin tapauksissa luoneet osastoja henkilöhallinnalle ja uusien kykyjen etsimiselle. Tämä malli jäljittelee etäisesti myös yritysmaailmassa tuttua Human Resources -osastoa.
- **Asiakaspalvelu:** Varsinkin kiristyshaittaohjelma-ryhmät ovat panostaneet asiakaspalveluun. Daniel Clayton kommentoi seuraavasti Slaten artikkelissa rikollisten asiakaspalvelua: **”Monet lunnasohjelmajengit vastaavat sähköpostiviesteihin muutamassa minuutissa tai tunnissa sen sijaan, että uhri joutuisi odottamaan päiviä.”** Claytonin mukaan joillakin on jopa puhelinpalvelukeskuksia, jotka tekevät maksamisesta helppoa (Steinnberg, S. 2022).
- **Taloushallinta:** Kryptovaluutta on usein rikollisryhmien pääsääntöinen valuutta. Kryptovaluutan käsittelylle on oma osastonsa, jonka tehtävänä on hallita lompakoita ja pestä varat tarvittavaan valuuttamuotoon.
- **Tutkimus-, kehittäminen ja innovaatio-osasto (RDI):** Verkkorikollisuus on nopeasti muuttuva ala, minkä vuoksi verkkorikollisorganisaatiot joutuvat panostamaan teknisiin asiantuntijoihin ja innovaattoreihin. Heidän tehtävänsä on kehittää ja ylläpitää työkaluja, kuten kiristyshaittaohjelmistoja, botnet-verkkoja tai kalastelusivustoja. Myös ohjelmistojen päivittäminen ja uusien versioiden tekeminen kuuluu heidän vastuulleen.

Euroopan unionin osarahoittama

XAMK
Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025

Asiantuntijan 1 avaa myös verkkorikollisryhmien rakennetta ottamalla esiin valtiolliset vaikuttajat. **”Osalla on tietysti ihan oma, tavallaan hyvin selkeä organisaatiollinen rakenne. Yhä etenevissä määrin kyse on enemmän siitä järjestäytyneestä rikollisuudesta, joka pystyy tavalla tai toisella myös palvelemaan vihamielistä valtiojohtoista toimintaa.”** Jos valtiolliset toimijat näkevät rikollisorganisaatioiden rakenteen yhtä vakaana kuin esimerkiksi heidän omat yksikkönsä, saadaan tarkempi kuva siitä mitä Suomella tai Suomen yrityksillä on vastassaan.

Asiantuntija 5 mukaan Venäjän hyökkäyssota Ukrainaan on pakotteiden ja rajoitteiden takia luonut Venäjän markkinoille teknologisen tyhjiön. Tämä tyhjiö on hidastanut uusien innovaatioiden kehittämistä ja rahoituksia: **”Venäjältä lähti paljon länsimaalaisia yrityksiä, joka loi sitten taas sinne tarpeen erinäköiselle teknologialle, tiedolle ja osaamiselle. Kun sitä ei ole saatavilla, niin mistä se sitten helpoiten saadaan, kuin varastamalla käytännössä.”** Ei ole ollenkaan kaukaa haettua uskoa, että Venäjän tiedustelupalvelut voivat käyttää erilaisia datan välittäjiä tai initial-access-toimijoita omissa operaatioissaan.

WithSecuren kyberrikollisuuden tutkimuspaperissa ilmoitetaan, että esimerkiksi Pohjois-Korean toimijat ovat ostaneet mahdollisia sisäänpääsyjä yritys- ja organisaatioverkkoinfrastruktuureihin (Withsecure whitepaper, 4).

5. Vaikutukset

Kyberuhkien muodostamat riskit ovat jo muodostuneet yrityksille keskeisiksi osaksi riskienhallintaa ja jatkuvuussuunnitelmaa. Mahdollisia riskejä/vaikutuksia voivat olla esimerkiksi:

- **Kasvanut kyberhyökkäysten riski**: Koska kyberrikollisuuteen mahdollistavien työkalujen ostaminen helpottaa verkkorikoksia, tulee hyökkäysten volyymi myös kasvamaan.
- **Hyökkäysten kohdentaminen pienempiin yrityksiin:** Mahdollisten huijaus- ja kalastelukampanjoiden volyymi, laatu sekä määrä voivat kasvaa kilpailullisten palveluiden tarjonnan seurauksena. Tämänkaltaisten kampanjoiden johdosta myös pienemmät yritykset voivat joutua huijausaallon kohteeksi.
- **Liiketoiminnan keskeytyminen:** Palvelunestohyökkäykset tai kiristyshaittaohjelmaiskut voivat estää yrityksen tai asiakkaiden pääsyn tärkeisiin järjestelmiin tai palveluihin. Tämä voi johtaa tuotannon tai palvelujen keskeytyksiin, jotka haittaavat yrityksen jokapäiväistä toimintaa ja voivat aiheuttaa haittoja taloudelle ja maineelle.
- **Tietovuodot:** Mahdolliset tietovuodot voivat olla yrityksen kaatava riski. Asiakas- tai sidosryhmien tietojen vuotaminen aiheuttaa minimissään mainehaittaa, sakkoja ja vakavimmillaan yrityksen kaatumisen.

Asiantuntija 1 mielestä As-a-Service-mallin toimintamuodot ovat vahvasti kasvussa, mikä pystytään näkemään suoranaisesti kybertoimintaympäristössä lisääntyvinä erilaisina hyökkäyksinä sekä onnistuneiden käyttäjätunnusten kalastelun määrän kasvuna. Menetetyt käyttäjätunnukset puolestaan johtivat esimerkiksi kiristyshaittaohjelmaryhmien hyökkäyksiin. Tämänkaltaisten hyökkäysten kohteina Suomessa on ollut esimerkiksi Tietoevry, Valtra, Suomen Tietotoimisto ja Westlog. Westlog-hyökkäyksien seurauksena yli 116 000 ihmisen tietoturva vaarantui (Uhari, M. 2023).

Euroopan unionin osarahoittama

Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025

Todennäköisyydet

Kuinka todennäköistä on, että yritys joutuu ammattimaisen kyberrikollisuuden uhriksi? Jos yritykseen tehdään jonkinasteinen kyberhyökkäys, on hyvinkin mahdollista, että kyseessä on ollut suuremman rikollisryhmän alihankkija tai suoraan yksi sen ”työntekijöistä.” Kun kyberrikoksia tehdään, on suurin osa niistä tavalla tai toisella yhteydessä järjestäytyneeseen rikollisuuteen. Nykyään on hyvin epätodennäköistä, että hyökkäävät verkkorikolliset tuottaisivat kaikki työkalut, haittaohjelmat ja kampanjat itse tai ryhmien tapauksissa ”in house”. Palvelumallien yleistymisen myötä rikollisten on helppouden lisäksi myös varmempaa käyttää muiden luomia palveluita. Usein taitavien toimijoiden valmistamat työkalut tai haittaohjelmat ovat tehokkaita juuri niissä tarkoituksissa, mihin ne on suunniteltu. Tämänkaltaisten työkalujen sekä haittaohjelmien tekeminen omin voimin on:

- **Henkilön taitotasosta riippuen erittäin vaikeaa.**
- **Vaikka työkalu tai haittaohjelma saadaan valmiiksi, ei se vielä varmista sen toimivuutta kaikissa ympäristöissä. Rikollisilla, joiden päätavoitteena on tehdä rahaa, ei juurikaan ole aikaa testata omaa ohjelmistoaan tai työkaluaan eri ympäristöissä.**
- **Taloudellisesti kannattavampaa on hankkia esimerkiksi haittaohjelman kuukausipalvelu. Tämä antaa rikolliselle valmiin sovelluksen, jota on helppo käyttää. Usein tähän myös kuuluu asiakaspalvelu joka neuvoo, kuinka toimia erilaisten hyökkäysten suhteen.**

Asiantuntija 5 mukaan Cybercrime-as-a-Service ilmentyy vahvasti siellä, missä taloudellista hyötyä on saatavilla: **”Parin vuoden selkeä kehityssuunta, esimerkiksi kiristyshaittaohjelmia suhteen, on sen toiminnan jakautuminen. Siellä missä on saatavilla paljon rahaa, niin silloin yleensä semmoiset erikoistoimijat osallistuvat tiettyihin operaatioihin, ja siihen koko hyökkäysketjuun tulee paljon enemmän sitten osapuolia mukaan.”** Tämän takia yksi suurempi tai useat pienemmät kyberhyökkäykset voivat sisältää useita eri jakautuneita ryhmiä osana hyökkäysketjua. Tämän seurauksena hyökkäyskaava on todella verkostoitunut, jonka takia on vaikea saada varmuutta siitä mikä on osa järjestäytyneempää rikollisryhmää ja mikä ei.

Kiristyshaittaohjelmaryhmät ovat lähes aina pääsääntöisesti taloudellisesti motivoituneita. Silloin kun kiristyshaittaohjelmat alkoivat yleistyä, olivat ensisijaisia uhreja loppukäyttäjät. Yksityishenkilön tietokone saattoi saastua sähköpostien liitetiedostojen tai linkkien kautta, ja tämän saastumisen takia tietokonetta ei voinut käyttää ennen kuin tarvittava rahasumma oli maksettu.

Asiantuntija 4 mukaan rikollisryhmät ovat ottaneet kohteikseen suuremmat yritykset, joilta kuusinumeroisten tai suurempien rahamäärien maksaminen onnistuu todennäköisemmin. Asiantuntija 4 ilmaisee, että pienemmät yritykset ovat itse asiassa vähän paremmin turvassa suurilta verkkorikollisilta juuri niiden pienen koon takia. Kuitenkin automatisoidut kalastelukampanjat ja hyökkäykset voivat osua kehen tahansa. Pienten yrittäjien ei tulisi tuudittautua ajatukseen, että heidän yrityksensä olisi liian pieni kiinnostaakseen rikollisia.

Pienemmät yritykset kiinnostavat rikollisia erityisesti niiden kytköksistä suurempiin yrityksiin, kuten alihankintasuhteiden kautta. Pienemmät yritykset voivat olla osa alihankintaketjuhyökkäystä, minkä takia suurempi yritys joutuu kyberhyökkäyksen kohteeksi niiden kautta.

Euroopan unionin osarahoittama

XAMK
Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

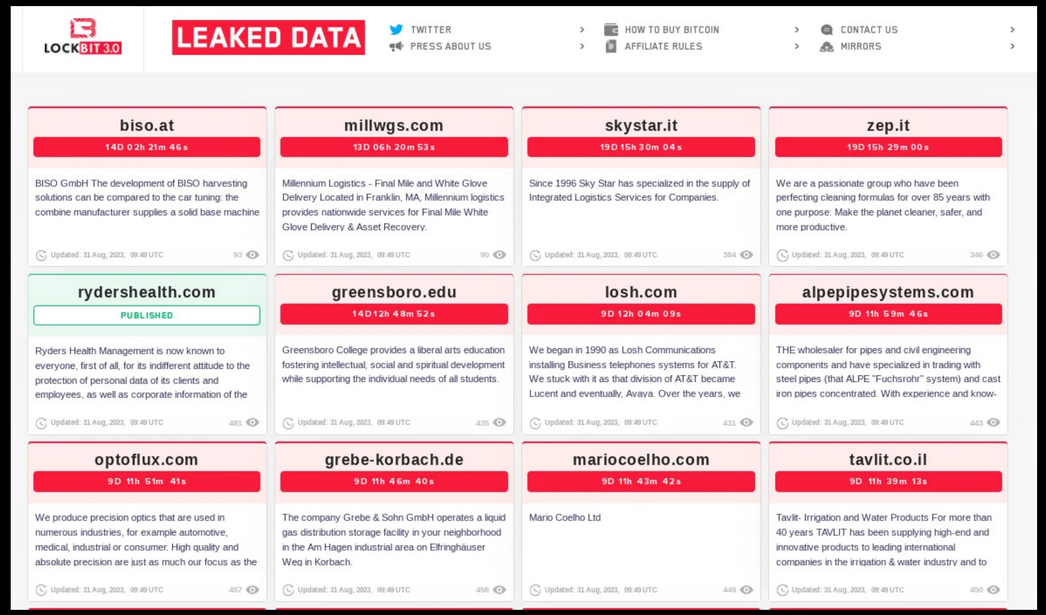
Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon



Kuva 10. LockBit-lunnashaittaohjelmaryhmän tietovuotokirjasto eri yrityksistä, julkaistut tiedot näkyvät vihreällä värillä (SOCRadar, 2023)

LockBitin ja Akiran kaltaiset lunnashaittaohjelmaryhmät operoivat pääsääntöisesti automatisoiduilla hyökkäyksillä. LockBit esimerkiksi kohdistaa automaattiset hyökkäyksensä usein myös ”Päivitystiistai (Patch Tuesday)”-nimisen päivän jälkeen, jolloin ryhmä saa tietoonsa mahdolliset laite- ja ohjelmistohaavoittuvuudet. LockBitin hyökkäykset kohdistuvat kaikkiin toimialoihin ja kaikenkokoisiin yrityksiin. LockBit salaa ja varastaa uhrin tiedot, joita he pitävät panttivankeina niin pitkään, kunnes lunnaat maksetaan. Jos lunnaita ei makseta määräaikaan mennessä, julkaistaan kaikki varastetut tiedot LockBitin nettisivuilla.

Kyberturvallisuuskeskuksen Heinäkuun Kybersäässä (Kyberturvallisuuskeskus. 2024). varoitettiin toimitus- ja palveluketjujen tietoturvan sekä jatkuvuuden kriittisyydestä. Organisaation tulee tuntea oman alihankintaketjunsa, sekä myös omien alihankkijayritystensä toiminta niin ohjelmisto- kuin verkkotasolla.

Euroopan unionin osarahoittama

Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025

6. Varautuminen

Kuinka sitten varautua CaaS:in tuomiin kyberhyökkäyksiin? Vastaus on yksinkertainen; toimenpiteet hyökkäysten estämiseksi eivät juurikaan muutu vanhoista kyber- ja tietoturvaopeista. Yritysten tulisi ylläpitää hyvää kyber- ja tietoturvaa samalla lailla kuin ennenkin. Asiantuntijat antoivat yrityksille hyviä neuvoja, joita voi ottaa käytäntöön, jos yrityksen tai organisaation kyberturva mietityttää:

- Asiantuntija 1 korostaa kyberkypsyyden tärkeyttä yritysmuodosta ja koosta riippumatta. Tällä tarkoitetaan yrityksen turvallisuuteen liittyvän asenteen eli kulttuurin parantamista kyber- ja tietoturvallisuus huomioiden.
- **”Kyber- ja tietoturvaa ei pidä nähdä vain yksittäisenä IT-osaston, yksikön tai yksittäisen ihmisen lokeroituna tehtävänä, vaan se koskettaa laajalti koko organisaatiota ja yritystä. Turvallisuuden “kruununjalokivi”-ajattelun pitäisi myös ulottua kyberturvaan.”**
- Asiantuntija 1 myös painottaa jatkuvuuden ja riskienhallinnan merkitystä yritystoiminnassa. Yritystoiminnan jatkuvuutta ei tulisi nähdä asiana, mikä tehdään kerran valmiiksi. Riskien tiedostaminen ja sitä kautta saatava riskien- ja jatkuvuudenhallinta on jatkuva prosessi, joka muuttaa muotoaan ajan sekä tilanteen mukaan.
- Kyberturvan tulevaisuus Kymenlaaksossa -hanke teki vuonna 2024 selvitystyön Kymenlaakson yritysten kyber- ja tietoturvan tilasta. Selvityksestä ilmeni, että 432 yrityksestä Kymenlaaksossa 69 % ei ollut tehnyt ollenkaan jatkuvuussuunnitelmaa omalle yritykselleen. Selvityksen pääset lukemaan tästä: **Kymenlaakson yritysten kyberturvakartoitus 2024 - Kyberasema %**
- Asiantuntija 3 haluaa yritysten ja organisaatioiden ottavan huomioon oman ulkoverkon kokonaiskuvan sekä sen mitä, kaikkea sisäverkko pitää sisällään. Tiivistetysti tämä tarkoittaa oman kotikentän perusteellista tuntemusta. Ottamalla selvää oman verkkoinfrastruktuurin laitteistosta, ohjelmistoista, konfiguraatioista ja mahdollisista IP-osoitteista, voidaan uhan tai hyökkäyksen sattuessa nopeuttaa vasteaikaa huomattavasti.
- Asiantuntija 3 myös ottaa tärkeänä seikkana esille päivittämisen ja haavoittumishallinnan. Yritysten ja organisaatioiden päivittämiskäytännöt tulisi olla mahdollisimman nopeasti toimivat, ja päivityksen julkaisun sekä asennuksen aikavälin ei tulisi olla liian pitkä.
- ”Tutkimuksessa vertailin haavoittumistiedotteita 4 vuoden ajalta. Viime vuoteen asti oli tehty 136 haavoittuvuustiedotetta. Niistä 60 % oli käytetty hyväksi kyberhyökkäyksissä ja tietomurroissa.”
- Asiantuntija 4 korostaa käyttövaltuuksien hallintaa yrityksissä ja organisaatioissa. Rajoittamalla pääsynhallintaa ja käyttäjäoikeuksia voidaan varmistaa, että vain valtuutetut henkilöt pääsevät käsiksi kriittisiin tietoihin ja järjestelmiin.
- Asiantuntija 5 mielestä yritysten tulisi panostaa varsinkin kalastelu- ja huijausviestien huomaamiseen.
- **”Phishing laatu, jota Suomeen tulee nykypäivänä, on aivan eri planeetalta kuin mitä vaikka 5 vuotta sitten. Jos se yrityksen ajatus esimerkiksi kalasteluun kanssa on se, että Suomessa ollaan edelleen vähän niin kuin lintukodossa ja huijaus- ja kalasteluviestit pystyy edelleen tunnistamaan kirjoitus- ja kielioppivirheistä, niin on se aika vanhentunut keino tämmöisten huomaamiseen.”**
- Myös turvallisuuskulttuurin tulisi olla mahdollisimman kannustava. Yrityksen työntekijöiden kyberhygienia koulutusta tulee vahvistaa, jotta voidaan parantaa ilmoittamisen ja tiedottamisen kulttuuria työyhteisössä.

Euroopan unionin osarahoittama

Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025

7. Johtopäätökset

Selvityksessä korostuu, että Crime-as-a-Service (CaaS) ja erityisesti Cybercrime-as-a-Service ovat jo olemassa olevia uhkia, jotka vaikuttavat monin tavoin yhteiskuntaan, talouteen ja turvallisuuteen. CaaS-mallin kautta kyberrikolliset saavat käyttöönsä työkaluja, teknologiaa ja palveluja, jotka madaltavat kynnystä toteuttaa monimutkaisia verkkorikoksia, kuten kiristysohjelmien levittämistä, tietomurtoja ja palvelunestohyökkäyksiä. Tämä mahdollistaa rikollisuuden kasvun ja sen laajentumisen myös teknisesti vähemmän osaaville henkilöille.

Yksi CaaS-ilmiön keskeinen seuraus on sen ammattimaistuminen: verkossa toimivat rikollisryhmät hyödyntävät liiketoiminnallisia rakenteita, kuten asiakaspalvelua, taloushallintoa ja jopa rekrytointia. Tämä rakenteellisuus tekee toiminnasta tehokasta ja hyvin tuottoisaa. Myös ryhmien hajautuneisuus tekee niistä joustavia, mikä hankaloittaa viranomaisten työtä niiden estämiseksi. Lisäksi teknologian kehittyminen ja helppokäyttöiset työkalut madaltavat kynnystä kokeilla tai ryhtyä verkkorikolliseen toimintaan, mikä houkuttelee nuoria ja kokemattomia tekijöitä mukaan kyberrikollisuuden kentälle. Samalla nämä organisaatiot kykenevät laajentamaan toimintaansa myymällä palveluja toisille rikollisille ja tarjoamalla heille tarvittavat työkalut.

Loppujen lopuksi Cybercrime-as-a-Servicen ja normaalin kyberrikollisuuden ero on kuin veteen piirretty viiva. On lähes mahdotonta erottaa, mikä osa verkkorikollisuudesta on osa kaupallista mallia ja mikä ei. Suurella todennäköisyydellä Cybercrime-as-a-Service-ilmiö on niin yleinen, että lähes kaikki verkkorikollisuus yhdistyy siihen tavalla tai toisella. Yritysten ja organisaatioiden ei tulisi ajatella CaaS-ilmiötä uutena uhkana, joka vaatisi uusia ja tehokkaita suojaustoimia. Pääsääntöisesti yrityksen kyberpuolustuksessa ei mikään muutu. Henkilökuntaa tulisi kouluttaa mahdollisten huijausten pääpiirteistä, ja yleistä kyberhygienia tulisi vahvistaa. Mahdollisen IT-tuen ja johtohenkilökunnan tulisi olla perillä yrityksen tai organisaation resursseista ja yrityksen sisäisestä verkkoinfrastruktuurista. Myös riskienarviointi, niiden hallinta ja jatkuvuussuunnitelma tulisi olla kunnossa tai siihen kannattaisi palata säännöllisin väliajoin.

Euroopan unionin osarahoittama

Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025

Lähteet

Chebac, A. 2023. What Is Cybercrime-as-a-Service (CaaS)?. Heimdal. WWW-dokumentti. Saatavissa: **https://heimdalsecurity.com/blog/what-is-cybercrime-as-a-service-caas/** [viitattu 12.9.2024]

Davidson, J., Aiken, M., Phillips, K., Farr, R. & Hanafiah, A. 2023. CC-DRIVER 2021 European Youth Survey. PDF-dokumentti. Saatavissa: **CC-DRIVER Policy Brief No. 8: European Youth Survey : UEL Research Repository** [viitattu 16.12.2024]

Fazzini, K. 2019. Cybercrime organizations work just like any other business: Here's what they do each day. CNBC. WWW-dokumentti. Saatavissa: **Here's what cybercriminals do during the workday** [viitattu 24.9.2024]

Kyberturvallisuuskeskus. 2024. Kybersää Heinäkuu 2024. Traficom Liikenne- ja viestintävirasto. PDF-dokumentti. Saatavilla: **Kybersää heinäkuu 2024.pdf** [viitattu 12.10.2024]

Matt, S. C., 2024. A defender's guide to crypters and loaders. red canary. WWW-dokumentti. Saatavissa: **A defender's guide to crypters and loaders | Red Canary** [viitattu 11.12.2024]

Slavin, B. 2024. What is Cybercrime-as-a-Service or CaaS?. DuoCircle. WWW-dokumentti. Saatavissa: **What is Cybercrime-as-a-Service or CaaS? - DuoCircle** [viitattu 12.9.2024]

SOCRadar. 2023. Dark Web Profile: LockBit 3.0 Ransomware. WWW-dokumentti. Saatavissa: **Dark Web Profile: LockBit 3.0 Ransomware - SOCRadar® Cyber Intelligence Inc.** [viitattu 12.12.2024]

SOCRadar. 2024. Top 10 Dark Web Markets. WWW-dokumentti. Saatavissa: **https://socradar.io/top-10-dark-web-markets/** [viitattu 7.10.2024]

Steinnberg, S. 2022. Ransomware Goes to Business School. SLATE. WWW-dokumentti. Saatavissa: **Why good customer service is key to ransomware scams.** [viitattu 23.9.2024]

Searchlight Cyber. 2023. Attack-For-Hire Services: The Evolution of DDoS. WWW-dokumentti. Saatavilla: **https://slcyber.io/attack-for-hire-services-the-evolution-of-ddos/** [viitattu 2.10.2024]

Sen, R. 2021. Here's how much your personal information is worth to cyber-criminals – and what they do with it. The Conversation. WWW-dokumentti. Saatavilla: **https://theconversation.com/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it-158934** [viitat-tu 8.10.2024]

Tillaeus, J. 2023. Jopa lapset tekevät palvelunestohyökkäyksiä – kohteena pelialustat ja koulumaailman Wilma. Yle. WWW-dokumentti. Saatavissa: **https://yle.fi/a/74-20059527** [viitattu 11.12.2024]

Uhari, M. 2023. Westlog-yhtiön tietomurto vaaransi yli 116 000 ihmisen tieto-turvan – laajuus moninkertainen Vastaamoon nähden. Iltasanomat. WWW-dokumentti. Saatavilla: **https://www.is.fi/digitoday/art-2000010031764.html** [viitattu 12.11.2024]

Euroopan unionin osarahoittama

Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025

Vardham, R. 2024. How Many Cyber Attacks Happen Per Day in 2024?. TechJury.
Saatavissa: https://techjury.net/blog/how-many-cyber-attacks-per-day/ [viitattu 9.10.2024]

WithSecure. The Professionalization of Cyber Crime | Whitepaper. PDF-dokumentti.
Saatavissa: WS_Professionalisation_of_CyberCrime_EN.pdf [viitattu 16.10.2024]

Zoltan, M. 2023. Dark Web Price Index 2023. PrivacyAffairs. WWW-dokumentti.
Saatavilla: Dark Web Price Index 2023 - Exclusive Research [viitattu 8.10.2024]

Kuvaluettelo

Euroopan unionin osarahoittama

Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Kyberturvan tulevaisuus Kymenlaaksossa

Selvitys

CaaS (Crime-as-a-Service) ilmiön vaikutus Kymenlaaksoon

Markus Hölsä

2025