Euroopan unionin
virallinen lehti

FI
L-sarja

2026/1713

13.7.2026

NEUVOSTON PÄÄTÖS (YUTP) 2026/1713,

annettu 13 päivänä heinäkuuta 2026,

unionia tai sen jäsenvaltioita uhkaavien kyberhyökkäysten vastaisista rajoittavista toimenpiteistä annetun päätöksen (YUTP) 2019/797 muuttamisesta

EUROOPAN UNIONIN NEUVOSTO, joka

ottaa huomioon Euroopan unionista tehdyn sopimuksen ja erityisesti sen 29 artiklan,

ottaa huomioon unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan ehdotuksen,

sekä katsoo seuraavaa:

(1) Neuvosto hyväksyi 17 päivänä toukokuuta 2019 päätöksen (YUTP) 2019/797 ([1]).

(2) Osana kestäviä, mukautettuja ja koordinoituja unionin toimia jatkuvan kyberuhkan muodostavia toimijoita vastaan kahdeksan luonnollista henkilöä ja neljä yhteisöä olisi lisättävä päätöksen (YUTP) 2019/797 liitteessä olevaan luetteloon luonnollisista henkilöistä, oikeushenkilöistä, yhteisöistä ja elimistä, joihin kohdistetaan rajoittavia toimenpiteitä. Kyseiset henkilöt ja yhteisöt ovat vastuussa vaikutukseltaan merkittävistä kyberhyökkäyksistä, jotka muodostavat ulkoisen uhan unionille tai sen jäsenvaltioille, tukevat niitä tai osallistuvat niihin.

(3) Päätös (YUTP) 2019/797 olisi sen vuoksi muutettava vastaavasti,

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

Muutetaan päätöksen (YUTP) 2019/797 liite tämän päätöksen liitteen mukaisesti.

2 artikla

Tämä päätös tulee voimaan päivänä, jona se julkaistaan *Euroopan unionin virallisessa lehdessä*.

Tehty Brysselissä 13 päivänä heinäkuuta 2026.

Neuvoston puolesta

Puheenjohtaja

K. KALLAS

([1]) Neuvoston päätös (YUTP) 2019/797, annettu 17 päivänä toukokuuta 2019, unionia tai sen jäsenvaltioita uhkaavien kyberhyökkäysten vastaisista rajoittavista toimenpiteistä (EUVL L 129 I, 17.5.2019, s. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

LIITE

Muutetaan päätöksen (YUTP) 2019/797 liite seuraavasti:

1) lisätään otsikon ”A. Luonnolliset henkilöt” alle merkinnät seuraavasti:

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
”20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ Peitenimet: ”Bentley”, ”Bergen”, ”Alex Konor”, ”Benny”, ”Ben”, ”Stern” Syntymäaika: 23.6.1988 Osoite: Serebristy Bulvar 34 (Serebristyy Bul’var); krp 1; flt 528; 197341; Pietari, Venäjän federaatio Kansalaisuus: venäläinen Sukupuoli: mies Lähellä olevat yhteisöt: TrickBot, Wizard Spider, Conti	Vitali Kovalev (Vitaly Kovalev) on johtohahmo Trickbot- ja Conti-haittaohjelmien osalta. Hänet tunnetaan verkossa myös nimillä ”Bentley”, ”Bergen”, ”Alex Konor”, ”Benny”, ”Ben” ja ”Stern”. Conti- ja Trickbot-haittaohjelmien alkuperäinen luoja ja kehittäjä on Wizard Spider. Wizard Spider on toteuttanut kiristysohjelmakampanjoita eri aloilla, liittyen muun muassa terveydenhuollon ja pankkitoiminnan kaltaisiin keskeisiin palveluihin, ja se on tartuttanut tietokoneita maailmanlaajuisesti, ja sen haittaohjelmia on kehitetty erittäin modulaariseksi haittaohjelmavalikoimaksi. Wizard Spiderin kampanjat, joissa käytetään Contin ja TrickBotin kaltaisia haittaohjelmia, ovat vastuussa huomattavasta taloudellisesta vahingosta Euroopan unionissa. Vitali Kovalev on näin ollen vastuussa vaikutukseltaan merkittävistä kyberhyökkäyksistä, jotka muodostavat ulkoisen uhan unionille tai sen jäsenvaltioille, ja osallistuu niihin.	13.7.2026

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Syntymäaika: 30.1.1983 Syntymäpaikka: SNTL Kansalaisuus: venäläinen Passin numero: 762988138 Sukupuoli: mies Lähellä olevat yhteisöt: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik on Media Land LLC:n omistaja. Bullet Proof Hosting Service Media Land LLC on vuodesta 2016 lähtien edistänyt monenlaisia haittaohjelmahyökkäyksiä sekä unionissa että maailmanlaajuisesti tarjoamalla säilytyspalveluja, jotka piilottavat käyttäjien henkilöllisyydet ja onnistuvat estämään lainvalvontaviranomaisten tekemät poistot. Media Land LLC on mahdollistanut laajamittaiset kiristysohjelmaoperaatiot, komento- ja valvontapalvelut sekä verkkourkintaoperaatiot, jotka kohdistuvat kriittiseen infrastruktuuriin ja keskeisiin palveluihin jäsenvaltioissa, mikä on johtanut merkittäviin taloudellisiin tappioihin. Media Land LLC:n tukemia operaatioita ovat muun muassa LockBit, EvilCorp ja BlackBasta. Sen vuoksi Media Land LLC on osallisena vaikutukseltaan merkittävissä kyberhyökkäyksissä, jotka muodostavat ulkoisen uhan unionille tai sen jäsenvaltioille. Media Land LLC:n omistajana Alexander Volosovik on vastuussa näistä kyberhyökkäyksistä ja osallistuu niihin. Hän on myös lähellä Media Land LLC:tä.	13.7.2026

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Alias: ”Dena” Syntymäaika: 9.10.1989 Syntymäpaikka: SNTL Kansalaisuus: venäläinen Sukupuoli: mies Osoite: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburgin alue, Venäjän federaatio	Denis Degtjarenko (Denis Degtyarenko), alias Dena, on venäläinen hakkeri CARR-järjestössä (Cyber Army of Russia Reborn). CARR on ollut vastuussa kyberhyökkäyksistä, jotka kohdistuvat palveluihin, jotka ovat tarpeen keskeisen taloudellisen toiminnan ja kriittisten valtion toimintojen ylläpitämiseksi jäsenvaltioissa, sekä Ukrainan ja muiden kolmansien maiden infrastruktuuriin. CARR on yhteydessä Venäjän federaation asevoimien yleisesikunnan pääosaston (GRU) erikoisteknologioiden pääkeskukseen (GTsST). GTsST toteuttaa edelleen aktiivisesti kyberhyökkäyksiä unionia ja sen jäsenvaltioita vastaan. CARR:n kohteita ovat muun muassa valtion virastot, rahoituslaitokset, tiedotusvälineet ja kriittinen infrastruktuuri jäsenvaltioissa ja Yhdysvalloissa. CARR on tehnyt hajautettuja palvelunestohyökkäyksiä Ukrainassa sekä Ukrainaa tukeneiden maiden hallituksia ja näissä maissa sijaitsevia yrityksiä vastaan. Sen vuoksi Denis Degtjarenko, yksi CARR:n päähakkereista, on osallisena vaikutukseltaan merkittävissä kyberhyökkäyksissä, mukaan lukien potentiaaliselta vaikutukseltaan merkittävien kyberhyökkäysten yritykset, jotka muodostavat ulkoisen uhan jäsenvaltioille sekä kolmansille valtioille. CARR:n jäsenenä hän on myös lähellä GTsST:tä.	13.7.2026

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Alias: ”YUliYA” Syntymäaika: 6.4.1984 Syntymäpaikka: SNTL Kansalaisuus: venäläinen Sukupuoli: nainen Osoite: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburgin alue, Venäjän federaatio	Julija Pankratova (Yuliya Pankratova) on venäläinen hakkeri, joka on työskennellyt CARR:n (Cyber Army of Russia Reborn) palveluksessa. Hän on sittemmin perustanut Z-Pentestin ja työskentelee edelleen sen parissa. CARR on ollut vastuussa kyberhyökkäyksistä, jotka kohdistuvat palveluihin, jotka ovat tarpeen keskeisen taloudellisen toiminnan ja kriittisten valtion toimintojen ylläpitämiseksi jäsenvaltioissa, sekä Ukrainan ja muiden kolmansien maiden infrastruktuuriin. CARR on yhteydessä Venäjän federaation asevoimien yleisesikunnan pääosaston (GRU) erikoisteknologioiden pääkeskukseen (GTsST). GTsST toteuttaa edelleen aktiivisesti kyberhyökkäyksiä unionia ja sen jäsenvaltioita vastaan. CARR:n kohteita ovat muun muassa valtion virastot, rahoituslaitokset, tiedotusvälineet ja kriittinen infrastruktuuri jäsenvaltioissa ja Yhdysvalloissa. CARR on tehnyt hajautettuja palvelunestohyökkäyksiä Ukrainassa sekä Ukrainaa tukeneiden maiden hallituksia ja näissä maissa sijaitsevia yrityksiä vastaan. Z-Pentest on vastuussa vaikutukseltaan merkittävistä kyberhyökkäyksistä, jotka ovat kohdistuneet muun muassa palveluihin, jotka ovat tarpeen keskeisten toimintojen ylläpitämiseksi jäsenvaltioissa. Sen vuoksi Julija Pankratova, yksi CARR:n ja Z-Pentestin päähakkereista, on osallisena vaikutukseltaan merkittävissä kyberhyökkäyksissä, mukaan lukien potentiaaliselta vaikutukseltaan merkittävien kyberhyökkäysten yritykset, jotka muodostavat ulkoisen uhan jäsenvaltioille sekä kolmansille valtioille. Hän on myös lähellä Z-Pentestiä.	13.7.2026

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Alias: ”Daugn0” Kansalaisuus: oletettavasti venäläinen Sukupuoli: mies	Maksim Voronin, alias Daugn0, osallistuu tiedon varastamiseen keskittyvän LummaC2-haittaohjelman (alias Lumma Infostealer, Lumma Stealer) kehittämiseen, jakeluun ja myyntiin. LummaC2 on haittaohjelmapalvelu (Malware-as-a-Service, MaaS), jota käytetään arkaluonteisten tietojen, selaintunnisteiden, kryptolompakoiden tai järjestelmätietojen varastamiseen, uusien haittaohjelmien käyttöönottoon tartunnan saaneissa laitteissa, kryptovaluuttavarkauksiin ja vakoilukampanjoihin. LummaC2-haittaohjelmia hyödyntäviä kyberhyökkäyksiä käyttävät myös taloudellisesti motivoituneet kyberuhkatoimijat, kuten Storm-113, Storm-1607, Storm-1674, Octo Tempest ja muut. LummaC2-haittaohjelmia on käytetty kyberhyökkäyksiin sellaisia kriittisiä valtion toimintoja ja palveluja vastaan, jotka ovat tarpeen jäsenvaltioiden keskeisten sosiaalisten ja taloudellisten toimintojen ylläpitämiseksi. LummaC2 oli vuosina 2024 ja 2025 yksi maailman käytetyimmistä välineistä tiedon varastamiseen. Sen vuoksi asemassaan LummaC2:n kehittäjänä, jakelijana ja myyjänä Maksim Voronin osallistuu vaikutukseltaan merkittäviin kyberhyökkäyksiin, jotka muodostavat ulkoisen uhan jäsenvaltioille, ja helpottaa niitä.	13.7.2026

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
25.	Maksim Aleksandrovich GORDIENKO alias Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Alias: ”Lummaseller” Kansalaisuus: oletettavasti venäläinen Sukupuoli: mies	Maksim Gordienko, alias Lummaseller, osallistuu LummaC2-haittaohjelmien (alias Lumma infostealer, Lumma Stealer) kehittämiseen ja jakeluun. LummaC2 on haittaohjelmapalvelu (Malware-as-a-Service, MaaS), jota käytetään arkaluonteisten tietojen, selaintunnisteiden, kryptolompakoiden tai järjestelmätietojen varastamiseen, uusien haittaohjelmien käyttöönottoon tartunnan saaneissa laitteissa, kryptovaluuttavarkauksiin ja vakoilukampanjoihin. LummaC2-haittaohjelmia hyödyntäviä kyberhyökkäyksiä käyttävät myös taloudellisesti motivoituneet kyberuhkatoimijat, kuten Storm-113, Storm-1607, Storm-1674, Octo Tempest ja muut. LummaC2-haittaohjelmia on käytetty kyberhyökkäyksiin sellaisia kriittisiä valtion toimintoja ja palveluja vastaan, jotka ovat tarpeen jäsenvaltioiden keskeisten sosiaalisten ja taloudellisten toimintojen ylläpitämiseksi. LummaC2 oli vuosina 2024 ja 2025 yksi maailman käytetyimmistä välineistä tiedon varastamiseen. Sen vuoksi asemassaan LummaC2:n kehittäjänä, jakelijana ja myyjänä Maksim Gordienko osallistuu vaikutukseltaan merkittäviin kyberhyökkäyksiin, jotka muodostavat ulkoisen uhan jäsenvaltioille, ja helpottaa niitä.	13.7.2026

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Syntymäaika: 25.1.1980 Syntymäpaikka: SNTL Kansalaisuus: venäläinen Sukupuoli: mies Lähellä olevat henkilöt: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Lähellä olevat yhteisöt: GRU:n yksikkö 29155, ”Impuls” LLC	Evgeni Bašev (Evgeniy Bashev) on Venäjän sotilastiedusteluvirasto GRU:n yksikön 29155 jäsen. Yksikössä hän tukee ja helpottaa vaikutukseltaan merkittäviä kyberhyökkäyksiä jäsenvaltioita vastaan muun muassa hallinnoimalla hakkerointiin käytettävää Aegon-palvelinta. Hän antaa erityisesti teknistä ja aineellista tukea GRU:n yksikön 29155 kyberhyökkäyksille ”Impulse” LLC-yrityksensä kautta; yritys on helpottanut operaatioiden peittämistä ja välittänyt infrastruktuuria ja maksuja, ja se hallinnoi kyberhyökkäyksissä käytettäviä teknisiä resursseja, myös palvelimia. Hän myös koordinoi GRU:n rakenteiden ja ulkoisten hakkeriverkostojen välistä yhteistyötä. Hänen edistämänsä kyberhyökkäykset ovat kohdistuneet valtiollisiin kriittisten toimintojen järjestelmiin ja palveluihin, joita tarvitaan keskeisten sosiaalisten tai taloudellisten toimintojen ylläpitämiseksi jäsenvaltioissa, erityisesti liikennealalla. GRU:n yksikkö 29155 kohdisti WhisperGate-kampanjan kautta hyökkäyksiä myös Ukrainan kriittiseen infrastruktuuriin. Sen vuoksi Evgeni Bašev antaa teknistä ja aineellista tukea vaikutukseltaan merkittäville kyberhyökkäyksille mukaan lukien potentiaaliselta vaikutukseltaan merkittäville hyökkäysten yrityksille, jotka muodostavat ulkoisen uhan jäsenvaltioille, sekä vaikutukseltaan merkittäville kyberhyökkäyksille kolmatta maata vastaan, tai on muulla tavoin osallisena niihin. Omistajana ja pääjohtajana hän on lähellä ”Impulse” LLC-yhtiötä. GRU:n yksikön 29155 jäsenenä hän on myös lähellä tätä yhteisöä.	13.7.2026

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Syntymäpaikka: Venäjän federaatio Kansalaisuus: venäläinen Sukupuoli: mies Lähellä olevat henkilöt: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Lähellä olevat yhteisöt: GRU:n yksikkö 29155	Roman Puntus on Venäjän sotilastiedusteluviraston GRU:n yksikön 29155 jäsen. Yksikössä hänellä on johtava rooli jäsenvaltioihin kohdistuvien vaikutukseltaan merkittävien kyberhyökkäysten järjestämisessä ja koordinoinnissa. Hän tukee myös yksikön sisäisten kybervalmiuksien kehittämistä, mukaan lukien henkilöstön, kuten hakkereiden ja ohjelmoijien, rekrytointi ja valvonta. Hän on perustanut peiteyhtiön ”Aegeon-Impulse”, jonka avulla hän on edistänyt kyberoperaatioiden logistista ja taloudellista toimintaa. Yksikkö on toteuttanut hänen koordinoimiaan kyberhyökkäyksiä, jotka ovat kohdistuneet valtiollisiin kriittisten toimintojen järjestelmiin ja palveluihin, joita tarvitaan keskeisten sosiaalisten tai taloudellisten toimintojen ylläpitämiseksi jäsenvaltioissa, erityisesti liikennealalla. GRU:n yksikkö 29155 kohdisti WhisperGate-kampanjan kautta hyökkäyksiä myös Ukrainan kriittiseen infrastruktuuriin. Sen vuoksi Roman Puntus on vastuussa vaikutukseltaan merkittävistä kyberhyökkäyksistä mukaan lukien potentiaaliselta vaikutukseltaan merkittävät hyökkäysten yritykset, jotka aiheuttavat ulkoisen uhan jäsenvaltioille, sekä vaikutukseltaan merkittävistä kyberhyökkäyksistä kolmansia valtioita vastaan, tai on muulla tavoin osallisena niihin. GRU:n yksikön 29155 jäsenenä hän on myös lähellä tätä yhteisöä.	13.7.2026”;

2) lisätään otsikon ”B. Oikeushenkilöt, yhteisöt ja elimet” alle merkinnät seuraavasti:

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
”8.	Media Land LLC	Osoite: Tsvetnochnaya st., 16 Litera P, Room 27 Moskovskaya Zastava Municipal District Pietari, 196006, Venäjän federaatio Yhteisötyyppi: osakeyhtiö Rekisteröintipaikka: Pietari Rekisteröintipäivä: 19.10.2015 Rekisterinumero: 1152536009900 Päätoimipaikka: Pietari, Venäjän federaatio Lähellä oleva yhteisö: ML.Cloud	Bullet Proof Hosting Service Media Land LLC on vuodesta 2016 lähtien edistänyt monenlaisia haittaohjelmahyökkäyksiä jäsenvaltioissa ja maailmanlaajuisesti tarjoamalla säilytyspalveluja, jotka piilottavat käyttäjien henkilöllisyydet ja onnistuvat estämään lainvalvontaviranomaisten tekemät poistot, mikä on johtanut merkittäviin taloudellisiin tappioihin. Media Land LLC on mahdollistanut laajamittaiset kiristysohjelmaoperaatiot, komento- ja valvontapalvelut sekä verkkourkintaoperaatiot, jotka kohdistuvat kriittiseen infrastruktuuriin ja keskeisiin palveluihin jäsenvaltioissa. Media Land LLC:n tukemia operaatioita ovat muun muassa LockBit, EvilCorp ja BlackBasta. Sen vuoksi Media Land LLC on osallisena vaikutukseltaan merkittävissä kyberhyökkäyksissä, jotka muodostavat ulkoisen uhan jäsenvaltioille.	13.7.2026

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
9.	ML.Cloud	Osoite: Brivibas iela 52, Riika, LV-1011, Latvia; Venäjän federaatio, Kazan, Peterburgskaya st. 52 Rekisteröintipaikka: Riika Lähellä oleva henkilö: Alexander Volosovik Muut lähellä olevat yhteisöt: Media Land LLC	ML.Cloud on Media Land LLC:n sisaryhtiö, joka tarjoaa teknisen infrastruktuurin Media Land LLC:lle. Bullet Proof Hosting Service Media Land LLC on vuodesta 2016 lähtien edistänyt monenlaisia haittaohjelmahyökkäyksiä jäsenvaltioissa ja maailmanlaajuisesti tarjoamalla säilytyspalveluja, jotka piilottavat käyttäjien henkilöllisyydet ja onnistuvat estämään lainvalvontaviranomaisten tekemät poistot, mikä on johtanut merkittäviin taloudellisiin tappioihin. Media Land LLC on mahdollistanut laajamittaiset kiristysohjelmaoperaatiot, komento- ja valvontapalvelut sekä verkkourkintaoperaatiot, jotka kohdistuvat kriittiseen infrastruktuuriin ja keskeisiin palveluihin jäsenvaltioissa. Media Land LLC:n tukemia operaatioita ovat muun muassa LockBit, EvilCorp ja BlackBasta. Sen vuoksi Media Land LLC on osallisena kyberhyökkäyksissä, jotka muodostavat vaikutukseltaan merkittävän ulkoisen uhan EU:n jäsenvaltioille. Sen vuoksi ML. Cloud tarjoaa teknistä tukea vaikutukseltaan merkittäviin kyberhyökkäyksiin, jotka muodostavat ulkoisen uhan jäsenvaltioille.	13.7.2026

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
10.	”Impuls” LLC	Общество с ограниченной ответственностью ”Импульс” Osoite: 344015, Venäjän federaatio, Rostovin alue, Rostov-na-Donu, ul. Eremenko, d. 56, k. 6, apt. 88 Yhteisötyyppi: osakeyhtiö Rekisteröintipaikka: Interdistrict Inspectorate of the Federal Tax Service No. 26, Rostovin alue, 344019, Rostov-na-Donu, ul. Myasnikova, d. 52/32, Venäjän federaatio Rekisteröintipäivä: 27.9.2010 Rekisterinumero: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Päätoimipaikka: Venäjän federaatio Lähellä olevat henkilöt: Evgeniy Bashev Lähellä olevat yhteisöt: GRU:n yksikkö 29155	”Impuls” LLC on venäläinen yritys, jonka omistaa Venäjän sotilastiedusteluviraston GRU:n yksikön 29155 jäsen Evgeni Viktorovitš Bašev (Evgeni Viktorovich Bashev). Yritys antaa teknistä ja aineellista tukea GRU:n yksikön 29155 toteuttamille ja yrittämille kyberhyökkäyksille. ”Impuls” LLC-yhtiö toimii erityisesti operatiivisena välittäjänä, joka mahdollistaa hakkerointiin liittyvän toiminnan harjoittamisen sellaisen yrityksen kautta, joka ei ole muodollisesti sidoksissa Venäjän valtioon. Se on edistänyt kyberhyökkäysten operatiivista peittämistä ja välittänyt infrastruktuuria ja maksuja, ja sen teknisen puolen yhteyksiin luetaan hakkerointitoimien tukena käytettävät palvelimet. ”Impuls” LLC-yritys on erityisesti mahdollistanut yhteistyön GRU:n rakenteiden ja ulkoisten hakkeriverkostojen välillä. ”Impuls” LLC-yrityksen edistämät kyberoperaatiot ovat kohdistuneet valtiollisiin kriittisiin toimintoihin ja palveluihin, jotka ovat tarpeen keskeisten sosiaalisten ja taloudellisten toimintojen ylläpitämiseksi jäsenvaltioissa, erityisesti liikennealalla. GRU:n yksikkö 29155 kohdisti WhisperGate-kampanjan kautta hyökkäyksiä myös Ukrainan kriittiseen infrastruktuuriin. Sen vuoksi ”Impuls” LLC-yritys antaa teknistä ja aineellista tukea vaikutukseltaan merkittäville kyberhyökkäyksille, jotka muodostavat ulkoisen uhan jäsenvaltioille, sekä vaikutukseltaan merkittäville kyberhyökkäyksille kolmatta maata vastaan, tai on muulla tavoin osallisena niihin.	13.7.2026

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
11.	Z-Pentest	Peitenimet: ”Z-Pentest Alliance”, ”Z-Alliance” Päätoimipaikka: Venäjän federaatio Lähellä olevat henkilöt: Yuliya Pankratova Lähellä olevat yhteisöt: Cyber Army of Russia/CARR X.com-tili: ZPentest (tili suljettu) Telegram-tili: Zpentestalliance	Z-Pentest on venäläismielinen hakkeriryhmä, joka koostuu CARR:n (Cyber Army of Russia Reborn) ja NoName057:n jäsenistä ja joka kohdistaa maailmanlaajuisia hyökkäyksiään kriittiseen infrastruktuuriin, erityisesti energia- ja vesialalla. Ryhmä kohdisti hyökkäyksen tanskalaiseen vesilaitokseen joulukuussa 2024. Sen vuoksi Z-Pentest on vastuussa vaikutukseltaan merkittävistä kyberhyökkäyksistä, jotka muodostavat ulkoisen uhan jäsenvaltioille.	13.7.2026”.