



Bryssel, 5. toukokuuta 2026
(OR. en)

7281/26

LIMITE

CORLX 271
CFSP/PESC 388
CYBER 113
JAI 338
FIN 406

SÄÄDÖKSET JA MUUT VÄLINEET

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

NEUVOSTON PÄÄTÖS (YUTP) 2026/...,

annettu ... päivänä ...kuuta ...,

**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) 2019/797¹.
- (2) Päätöstä (YUTP) 2019/797 sovelletaan 18 päivään toukokuuta 2028.
- (3) Päätöksen (YUTP) 2019/797 liitteen uudelleentarkastelun pohjalta kyseisen päätöksen 4 ja 5 artiklassa säädettyjen toimenpiteiden soveltamista kyseisessä liitteessä lueteltuihin luonnollisiin henkilöihin, oikeushenkilöihin, yhteisöihin ja elimiin olisi jatkettava 18 päivään toukokuuta 2027. Lisäksi olisi saatettava ajan tasalle perusteet neljän henkilön ja yhden yhteisön merkitsemiselle luetteloon luonnollisista henkilöistä, oikeushenkilöistä, yhteisöistä ja elimistä, joihin kohdistetaan rajoittavia toimenpiteitä.
- (4) Päätös (YUTP) 2019/797 olisi sen vuoksi muutettava vastaavasti,

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

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

1 artikla

Muutetaan päätös (YUTP) 2019/797 seuraavasti:

1) korvataan 10 artikla seuraavasti:

”10 artikla

Tätä päätöstä sovelletaan 18 päivään toukokuuta 2028, ja sitä tarkastellaan jatkuvasti uudelleen. Edellä 4 ja 5 artiklassa säädettyjä toimenpiteitä sovelletaan liitteessä lueteltuihin luonnollisiin henkilöihin, oikeushenkilöihin, yhteisöihin ja elimiin 18 päivään toukokuuta 2027.”;

2) muutetaan liite tämän päätöksen liitteen mukaisesti.

2 artikla

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

Tehty ...ssa/ssä ... päivänä ...kuuta ...

Neuvoston puolesta

Puheenjohtaja

LIITE

Muutetaan päätöksen (YUTP) 2019/797 liite seuraavasti:

- 1) korvataan otsikon ”A. Luonnolliset henkilöt” alla olevat merkinnät 1, 2, 13 ja 14 seuraavilla vastaavilla merkinnöillä:

	Nimi	Tunnistustiedot	Luetteloon merkitsemisen perusteet	Luetteloon merkitsemisen päivämäärä
”1.	GAO Qiang	Syntymäaika: 4. lokakuuta 1983 Syntymäpaikka: Shandongin maakunta, Kiina Osoite: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, Kiina Kansalaisuus: kiinalainen Sukupuoli: mies	<p>Gao Qiang liittyy ”APT10” (”Advanced Persistent Threat 10”) -yhteisöön (alias ”Red Apollo”, ”CVNX”, ”Stone Panda”, ”MenuPass” ja ”Potassium”) ja on osallistunut ”Operation Cloud Hopper” -nimellä tunnettuun sarjaan vaikutukseltaan merkittäviä kyberhyökkäyksiä, jotka ovat peräisin unionin ulkopuolelta ja jotka muodostavat unionille tai sen jäsenvaltioille ulkoisen uhkan, ja vaikutukseltaan merkittäviä kyberhyökkäyksiä kolmansiä valtioita vastaan.</p> <p>”Operation Cloud Hopper” -kyberhyökkäysten kohteena ovat olleet monikansallisten yhtiöiden tietojärjestelmät kuudella mantereella, mukaan lukien unionissa sijaitsevat yhtiöt; hyökkäyksissä päästiin luvattomasti kaupallisesti arkaluonteisiin tietoihin, mistä aiheutui huomattavaa taloudellista tappiota.</p> <p>Gao Qiangilla on yhteyksiä APT10:n johtamis- ja valvontarakenteeseen. Lisäksi Gao Qiang on työskennellyt APT10:n käyttämässä Huaying Haitai -yhtiössä, joka on nimetty yhteisöksi, joka antaa tukea ”Operation Cloud Hopper” -kyberhyökkäyksille ja helpottaa niiden toteuttamista. Hänellä on myös yhteyksiä Zhang Shilongiin, joka liittyy APT10:een ja joka on myös ollut Huaying Haitain palveluksessa.</p>	30.7.2020

	Nimi	Tunnistustiedot	Luetteloon merkitsemisen perusteet	Luetteloon merkitsemisen päivämäärä
2.	ZHANG Shilong	<p>Syntymäaika: 10. syyskuuta 1981</p> <p>Syntymäpaikka: Kiina</p> <p>Osoite: Hedong, Yuyang Road No 121, Tianjin, Kiina</p> <p>Kansalaisuus: kiinalainen</p> <p>Sukupuoli: mies</p>	<p>Zhang Shilong liittyy ”APT10” (”Advanced Persistent Threat 10”) -yhteisöön (alias ”Red Apollo”, ”CVNX”, ”Stone Panda”, ”MenuPass” ja ”Potassium”) ja on osallistunut ”Operation Cloud Hopper” -nimellä tunnettuun sarjaan vaikutukseltaan merkittäviä kyberhyökkäyksiä, jotka ovat peräisin unionin ulkopuolelta ja jotka muodostavat unionille tai sen jäsenvaltioille ulkoisen uhkan, ja vaikutukseltaan merkittäviä kyberhyökkäyksiä kolmansia valtioita vastaan.</p> <p>”Operation Cloud Hopper” -kyberhyökkäysten kohteena ovat olleet monikansallisten yhtiöiden tietojärjestelmät kuudella mantereella, mukaan lukien unionissa sijaitsevat yhtiöt; hyökkäyksissä päästiin luvattomasti kaupallisesti arkaluonteisiin tietoihin, mistä aiheutui huomattavaa taloudellista tappiota.</p> <p>Zhang Shilong on lähellä APT10:tä, myös hänen APT10:n toteuttamien kyberhyökkäysten yhteydessä kehittämänsä ja testaamansa haittaohjelman kautta.</p> <p>Lisäksi Zhang Shilong on työskennellyt APT10:n käyttämässä Huaying Haitai -yhtiössä, joka on nimetty yhteisöksi, joka antaa tukea ”Operation Cloud Hopper” -kyberhyökkäyksille ja helpottaa niiden toteuttamista.</p> <p>Hän on lähellä Gao Qiangia, joka liittyy APT10:een ja joka on myös ollut Huaying Haitain palveluksessa.</p>	30.7.2020

	Nimi	Tunnistustiedot	Luetteloon merkitsemisen perusteet	Luetteloon merkitsemisen päivämäärä
13.	Mikhail Mikhailovich TSAREV	<p>Михаил Михайлович ЦАРЕВ</p> <p>Syntymäaika: 20.4.1989</p> <p>Syntymäpaikka: Serpuhov, Venäjän federaatio</p> <p>Kansalaisuus: venäläinen</p> <p>Osoite: Serpuhov</p> <p>Sukupuoli: mies</p>	<p>Mikhail Mikhailovich Tsarev osallistui vaikutukseltaan merkittäviin kyberhyökkäyksiin, jotka muodostavat ulkoisen uhkan EU:n jäsenvaltioille.</p> <p>Mihail Mikhailovich Tsarev, joka tunnetaan verkossa myös nimillä ”Mango”, ”Alexander Grachev”, ”Super Misha”, ”Ivanov Mixail”, ”Misha Krutysha” ja ”Nikita Andreevich Tsarev” on keskeinen toimija ”Conti”- ja ”Trickbot”-haittaohjelmien käytössä ja on osallistunut Venäjälle sijoittautuneeseen ”Wizard Spider” -ryhmään. Wizard Spider kehittää ja tehostaa toimintaansa edelleen.</p> <p>Wizard Spider on luonut Conti- ja Trickbot-haittaohjelmat ja kehittänyt niitä. Wizard Spider on toteuttanut kiristysohjelmakampanjoita useilla eri aloilla, muun muassa terveydenhuollon ja pankkitoiminnan kaltaisia välttämättömiä palveluja vastaan.</p> <p>Ryhmä on tartuttanut tietokoneita maailmanlaajuisesti, ja sen haittaohjelmia on kehitetty erittäin modulaariseksi haittaohjelmavalikoimaksi. Wizard Spiderin kampanjat, joissa käytetään Contin, ”Ryukin”, TrickBotin tai Black Bastan kaltaisia haittaohjelmia, aiheuttavat huomattavaa taloudellista vahinkoa Euroopan unionissa.</p> <p>Sen vuoksi Mikhail Mikhailovich Tsarev on osallistunut vaikutuksiltaan merkittäviin kyberhyökkäyksiin, jotka muodostavat ulkoisen uhkan unionille tai sen jäsenvaltioille.</p>	24.6.2024

	Nimi	Tunnistustiedot	Luetteloon merkitsemisen perusteet	Luetteloon merkitsemisen päivämäärä
14.	Maksim Sergeevich GALOCHKIN	<p>Максим Сергеевич ГАЛОЧКИН</p> <p>Syntymäaika: 19.5.1982</p> <p>Syntymäpaikka: Abakan, Venäjän federaatio</p> <p>Kansalaisuus: venäläinen</p> <p>Sukupuoli: mies</p>	<p>Maksim Galochkin osallistui vaikutukseltaan merkittäviin kyberhyökkäyksiin, jotka muodostavat ulkoisen uhkan EU:n jäsenvaltioille.</p> <p>Maksim Galochkin tunnetaan verkossa myös nimillä ”Benalen”, ”Bentley”, ”Volhvb”, ”volhvb”, ”manuel”, ”Max17” ja ”Crypt”. Galochkin on keskeinen toimija ”Conti”- ja ”Trickbot”-haittaohjelmien käytössä ja on osallistunut Venäjälle sijoittautuneeseen ”Wizard Spider” -ryhmään. Hän on johtanut joukkoa testaajia, joiden vastuulla on kehittää, valvoa ja toteuttaa testausta Wizard Spiderin luomaa ja käyttämää TrickBot-haittaohjelmaa varten. Wizard Spider kehittää ja tehostaa toimintaansa edelleen.</p> <p>Wizard Spider on toteuttanut kiristysohjelmakampanjoita useilla eri aloilla, muun muassa terveydenhuollon ja pankkitoiminnan kaltaisia välttämättömiä palveluja vastaan. Ryhmä on tartuttanut tietokoneita maailmanlaajuisesti, ja sen haittaohjelmia on kehitetty erittäin modulaariseksi haittaohjelmavalikoimaksi. Wizard Spiderin kampanjat, joissa käytetään Contin, ”Ryukin”, TrickBotin tai Black Bastan kaltaisia haittaohjelmia, aiheuttavat huomattavaa taloudellista vahinkoa Euroopan unionissa.</p> <p>Sen vuoksi Maksim Galochkin on osallistunut vaikutuksiltaan merkittäviin kyberhyökkäyksiin, jotka muodostavat ulkoisen uhkan unionille tai sen jäsenvaltioille.</p>	24.6.2024”;

2) korvataan otsikon ”B. Oikeushenkilöt, yhteisöt ja elimet” alla oleva merkintä 1 seuraavasti:

	Nimi	Tunnistustiedot	Luetteloon merkitsemisen perusteet	Luetteloon merkitsemisen päivämäärä
”1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	alias: Haitai Technology Development Co. Ltd Toimipaikka: Tianjin, Kiina	<p>Huaying Haitai -yhtiö antoi taloudellista, teknistä tai aineellista tukea ja helpotti toimia, jotka liittyivät ”Operation Cloud Hopper” nimellä tunnettuun sarjaan vaikutukseltaan merkittäviä kyberhyökkäyksiä, jotka ovat peräisin unionin ulkopuolelta ja jotka muodostavat unionille tai sen jäsenvaltioille ulkoisen uhkan, ja vaikutukseltaan merkittäviä kyberhyökkäyksiä kolmansia valtioita vastaan.</p> <p>”Operation Cloud Hopper” -kyberhyökkäysten kohteena ovat olleet monikansallisten yhtiöiden tietojärjestelmät kuudella mantereella, mukaan lukien unionissa sijaitsevat yhtiöt; hyökkäyksissä päästiin luvattomasti kaupallisesti arkaluonteisiin tietoihin, mistä aiheutui huomattavaa taloudellista tappiota.</p> <p>”Operation Cloud Hopper” -kyberhyökkäykset toteutti toimija, joka julkisuudessa tunnetaan nimellä ”APT10” (”Advanced Persistent Threat 10”) (alias ”Red Apollo”, ”CVNX”, ”Stone Panda”, ”MenuPass” ja ”Potassium”).</p> <p>Huaying Haitai -yhtiö voidaan yhdistää APT10:een. Lisäksi Huaying Haitai -yhtiössä työskentelivät Gao Qiang ja Zhang Shilong, jotka molemmat on nimetty ”Operation Cloud Hopper” -kyberhyökkäysten yhteydessä. Huaying Haitai -yhtiöllä on siis myös yhteyksiä Gao Qiangiin ja Zhang Shilongiin.</p>	30.7.2020”.