2024/1390

17.5.2024

IZVEDBENA UREDBA SVETA (EU) 2024/1390

z dne 17. maja 2024

o izvajanju Uredbe (EU) 2019/796 o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo Unijo ali njene države članice

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe Sveta (EU) 2019/796 z dne 17. maja 2019 o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo Unijo ali njene države članice [1] in zlasti člena 13(1) Uredbe,

ob upoštevanju predloga visokega predstavnika Unije za zunanje zadeve in varnostno politiko,

ob upoštevanju naslednjega:

(1) Svet je 17. maja 2019 sprejel Uredbo (EU) 2019/796.

(2) Glede na stalne in vse pogostejše zlonamerne kibernetske dejavnosti, vključno z dejavnostmi, usmerjenimi proti tretjim državam, bi bilo treba posodobiti razloge za uvrstitev šestih oseb in dveh subjektov na seznam fizičnih in pravnih oseb, subjektov in organov, za katere veljajo omejevalni ukrepi, iz Priloge I k Uredbi (EU) 2019/796.

(3) Prilogo I k Uredbi (EU) 2019/796 bi bilo zato treba ustrezno spremeniti –

SPREJEL NASLEDNJO UREDBO:

Člen 1

Priloga I k Uredbi (EU) 2019/796 se spremeni v skladu s Prilogo k tej uredbi.

Člen 2

Ta uredba začne veljati dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 17. maja 2024

Za Svet

predsednica

H. LAHBIB

[1] UL L 129 I, 17.5.2019, str. 1.

PRILOGA

Priloga I k Uredbi (EU) 2019/796 („Seznam fizičnih in pravnih oseb, subjektov in organov iz člena 3“) se spremeni:

(1) na seznamu z naslovom „A. Fizične osebe“ se vnosi 3 do 8 nadomestijo z naslednjim:

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
„3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Datum rojstva: 27.5.1972 Kraj rojstva: oblast Perm, Ruska SFSR (zdaj Ruska federacija) Številka potnega lista: 120017582 Izdajatelj: Ministrstvo za zunanje zadeve Ruske federacije Veljavnost: od 17.4.2017 do 17.4.2022 Lokacija: Moskva, Ruska federacija Državljanstvo: rusko Spol: moški	Sodeloval je pri poskusu kibernetskega napada s potencialno pomembnim učinkom na Organizacijo za prepoved kemičnega orožja (OPCW) na Nizozemskem in pri kibernetskih napadih s pomembnim učinkom na tretje države. Kot pomožni uradnik za HUMINT (zbiranje obveščevalnih podatkov z osebnimi stiki) v Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil eden izmed štirih članov skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila 2018 poskušala pridobiti nepooblaščen dostop do brezžičnega omrežja OPCW v Haagu (Nizozemska). Cilj poskusa kibernetskega napada je bil vdor v brezžično omrežje OPCW, pri čemer bi, če bi poskus uspel,to ogrozilo varnost omrežja in tekoče preiskovalno delo OPCW. Nizozemska varnostna služba za zaščito in varnost (Militaire Inlichtingen- en Veiligheidsdienst) je poskus kibernetskega napada ustavila in s tem preprečila resno škodo za OPCW. Velika porota v zahodnem okrožju Pensilvanije (Združene države Amerike) je Minina kot častnika ruskega glavnega obveščevalnega direktorata (GRU) obtožila zaradi vdora v računalniški sistem, goljufije z uporabo telekomunikacij, hujše kraje identitete in pranja denarja.	30.7.2020

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Datum rojstva: 31.7.1977 Kraj rojstva: oblast Murmanskaya, Ruska SFSR (zdaj Ruska federacija) Številka potnega lista: 100135556 Izdajatelj: Ministrstvo za zunanje zadeve Ruske federacije Veljavnost: od 17.4.2017 do 17.4.2022 Lokacija: Moskva, Ruska federacija Državljanstvo: rusko Spol: moški	Sodeloval je pri poskusu kibernetskega napada s potencialno pomembnim učinkom na Organizacijo za prepoved kemičnega orožja (OPCW) na Nizozemskem in pri kibernetskih napadih s pomembnim učinkom na tretje države. Kot kibernetski operater v Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil eden izmed štirih članov skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila 2018 poskušala pridobiti nepooblaščen dostop do brezžičnega omrežja OPCW v Haagu (Nizozemska). Cilj poskusa kibernetskega napada je bil vdor v brezžično omrežje OPCW pri čemer bi, če bi poskus uspel, to ogrozilo varnost omrežja in tekoče preiskovalno delo OPCW. Nizozemska varnostna služba za zaščito in varnost (Militaire Inlichtingen- en Veiligheidsdienst) je poskus kibernetskega napada ustavila in s tem preprečila resno škodo za OPCW. Velika porota v zahodnem okrožju Pensilvanije (Združene države Amerike) je Morenetsa, dodeljenega ‚vojaški enoti 26165‘, obtožila zaradi vdora v računalniški sistem, goljufije z uporabo telekomunikacij, hujše kraje identitete in pranja denarja.	30.7.2020

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Datum rojstva: 26.7.1981 Kraj rojstva: Kursk, Ruska SFSR (zdaj Ruska federacija) Številka potnega lista: 100135555 Izdajatelj: Ministrstvo za zunanje zadeve Ruske federacije Veljavnost: od 17.4.2017 do 17.4.2022 Lokacija: Moskva, Ruska federacija Državljanstvo: rusko Spol: moški	Sodeloval je pri poskusu kibernetskega napada s potencialno pomembnim učinkom na Organizacijo za prepoved kemičnega orožja (OPCW) na Nizozemskem in pri kibernetskih napadih s pomembnim učinkom na tretje države. Kot kibernetski operater v Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil eden izmed štirih članov skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila 2018 poskušala pridobiti nepooblaščen dostop do brezžičnega omrežja OPCW v Haagu (Nizozemska). Cilj poskusa kibernetskega napada je bil vdor v brezžično omrežje OPCW pri čemer bi, če bi poskus uspel, to ogrozilo varnost omrežja in tekoče preiskovalno delo OPCW. Nizozemska varnostna služba za zaščito in varnost (Militaire Inlichtingen- en Veiligheidsdienst) je poskus kibernetskega napada ustavila in s tem preprečila resno škodo za OPCW. Od pomladi leta 2022 vodi akterja in hekersko skupino ‚Sandworm' (tudi ‚Sandworm Team', ‚BlackEnergy Group', ‚Voodoo Bear', ‚Quedagh', ‚Olympic Destroyer' in ‚Telebots'), ki je povezana z enoto 74455 ruskega glavnega obveščevalnega direktorata. Skupina Sandworm po vojni agresiji Rusije proti Ukrajini izvaja kibernetske napade na Ukrajino, med drugim tudi na ukrajinske vladne agencije.	30.7.2020

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Datum rojstva: 24.8.1972 Kraj rojstva: Ulyanovsk, Ruska SFSR (zdaj Ruska federacija) Številka potnega lista: 120018866 Izdajatelj: Ministrstvo za zunanje zadeve Ruske federacije Veljavnost: od 17.4.2017 do 17.4.2022 Lokacija: Moskva, Ruska federacija Državljanstvo: rusko Spol: moški	Sodeloval je pri poskusu kibernetskega napada s potencialno pomembnim učinkom na Organizacijo za prepoved kemičnega orožja (OPCW) na Nizozemskem in pri kibernetskih napadih s pomembnim učinkom na tretje države. Kot pomožni uradnik za HUMINT (zbiranje obveščevalnih podatkov z osebnimi stiki) v Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil eden izmed štirih članov skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila 2018 poskušala pridobiti nepooblaščen dostop do brezžičnega omrežja OPCW v Haagu (Nizozemska). Cilj poskusa kibernetskega napada je bil vdor v brezžično omrežje OPCW pri čemer bi, če bi poskus uspel, to ogrozilo varnost omrežja in tekoče preiskovalno delo OPCW. Nizozemska varnostna služba za zaščito in varnost (Militaire Inlichtingen- en Veiligheidsdienst) je poskus kibernetskega napada ustavila in s tem preprečila resno škodo za OPCW. Velika porota v zahodnem okrožju Pensilvanije je Sotnikova kot častnika ruskega glavnega obveščevalnega direktorata (GRU) obtožila zaradi vdora v računalniški sistem, goljufije z uporabo telekomunikacij, hujše kraje identitete in pranja denarja.	30.7.2020

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Datum rojstva: 15.11.1990 Kraj rojstva: Kursk, Ruska SFSR (zdaj Ruska federacija) Državljanstvo: rusko Spol: moški	Sodeloval je v kibernetskem napadu s pomembnim učinkom proti nemškemu zveznemu parlamentu (Deutscher Bundestag) in pri kibernetskih napadih s pomembnim učinkom na tretje države. Kot vojaški obveščevalni uradnik 85. glavnega centra za posebne storitve (GTsSS) Glavnega direktorata generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil član skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila in maja leta 2015 izvedla kibernetski napad na nemški zvezni parlament. Cilj tega kibernetskega napada je bil informacijski sistem parlamenta, katerega delovanje je bilo nato več dni prizadeto. Ukradena je bila znatna količina podatkov, prav tako pa so bili prizadeti e-poštni računi več poslancev ter nekdanje kanclerke Angele Merkel. Velika porota v zahodnem okrožju Pensilvanije (Združene države Amerike) je Badina, dodeljenega ‚vojaški enoti 26165‘, obtožila zaradi vdora v računalniški sistem, goljufije z uporabo telekomunikacij, hujše kraje identitete in pranja denarja.	22.10.2020

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Datum rojstva: 21.2.1961 Državljanstvo: rusko Spol: moški	Trenutno je vodja Glavnega direktorata generalštaba Oboroženih sil Ruske federacije (GU/GRU), pred tem pa je bil prvi namestnik vodje. Ena od enot pod njegovim poveljstvom je 85. glavni center za posebne storitve (GTsSS), (tudi ‚vojaška enota 26165', ‚APT28', ‚Fancy Bear', ‚Sofacy Group', ‚Pawn Storm' in ‚Strontium'). V tej vlogi je odgovoren za kibernetske napade, ki jih je izvedel GTsSS, tudi tiste s pomembnim učinkom, ki pomenijo zunanjo grožnjo Uniji ali njenim državam članicam. Vojaški obveščevalni uradniki GTsSS so sodelovali zlasti v kibernetskem napadu na nemški zvezni parlament (Deutscher Bundestag) v aprilu in maju leta 2015, in v poskusu kibernetskega napada, katerega cilj je bil vdor v brezžično omrežje Organizacije za prepoved kemičnega orožja (OPCW) na Nizozemskem aprila 2018. Cilj kibernetskega napada na nemški zvezni parlament je bil informacijski sistem parlamenta, katerega delovanje je bilo nato več dni prizadeto. Ukradena je bila znatna količina podatkov, prav tako pa so bili prizadeti e-poštni računi več poslancev ter nekdanje kanclerke Angele Merkel.	22.10.2020“;

(2) na seznam z naslovom „B. Pravne osebe, subjekti in organi“ se vnosa 3 in 4 nadomestita z naslednjim:

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
„3.	Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Naslov: 22 Kirova Street, Moscow, Russian Federation	Center, znan tudi kot poštni predal 74455, je vpleten v kibernetske napade s pomembnim učinkom, ki se izvajajo zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetske napade, ki imajo pomemben učinek na tretje države, vključno s kibernetskima napadoma junija 2017, v javnosti znanima kot ‚NotPetya‘ ali ‚EternalPetya‘, in kibernetskimi napadi na ukrajinsko električno omrežje pozimi leta 2015 in 2016. ‚NotPetya‘ ali ‚EternalPetya‘ sta z izsiljevalskim virusom in onemogočenjem dostopa do podatkov onemogočila dostop do podatkov v številnih družbah v Uniji, širši Evropi in po svetu, kar je med drugim povzročilo precejšnjo ekonomsko izgubo. Zaradi kibernetskega napada na ukrajinsko električno omrežje je pozimi prišlo do delnega izpada tega omrežja. ‚NotPetya‘ ali ‚EternalPetya‘ je izvedel akter, v javnosti znan kot ‚Sandworm‘ (tudi ‚Sandworm Team‘, ‚BlackEnergy Group‘, ‚Voodoo Bear‘, ‚Quedagh‘, ‚Olympic Destroyer‘ in ‚Telebots‘), ki je odgovoren tudi za napad na ukrajinsko električno omrežje. Sandworm po vojni agresiji Rusije proti Ukrajini izvaja kibernetske napade na Ukrajino, med drugim tudi na ukrajinske vladne agencije in ukrajinsko kritično infrastrukturo. Ti kibernetski napadi vključujejo kampanje kibernetskih napadov na posameznike (spear-phishing) ter napade z zlonamerno programsko opremo in z izsiljevalskim programjem. Center dejavno sodeluje pri kibernetskih dejavnostih, ki jih izvaja Sandworm, in ga je mogoče povezati s Sandwormom.	30.7.2020

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
4.	85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Naslov: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation	Center, (tudi ‚vojaška enota 26165', ‚APT28', ‚Fancy Bear', ‚Sofacy Group', ‚Pawn Storm' in ‚Strontium') je vpleten v kibernetske napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetske napade, ki imajo pomemben učinek na tretje države. Vojaški obveščevalni uradniki GTsSS so sodelovali zlasti v kibernetskem napadu na nemški zvezni parlament (Deutscher Bundestag) v aprilu in maju leta 2015, in v poskusu kibernetskega napada, katerega cilj je bil vdor v brezžično omrežje Organizacije za prepoved kemičnega orožja (OPCW) na Nizozemskem v aprilu leta 2018. Cilj kibernetskega napada na nemški zvezni parlament je bil informacijski sistem parlamenta, katerega delovanje je bilo nato več dni prizadeto. Ukradena je bila znatna količina podatkov, prav tako pa so bili prizadeti e-poštni računi več poslancev ter nekdanje kanclerke Angele Merkel. Po vojni agresiji Rusije proti Ukrajini je GTsSS na Ukrajino izvedeli kibernetske napade (kibernetske napade na posameznike (spearphishing) in napade z zlonamerno programsko opremo).	22.10.2020“